Euler systems and the Bloch–Kato conjecture

David Loeffler
(UniDistance Suisse)

Mathematics Münster Mid-term Conference

Münster, 27/3/2024

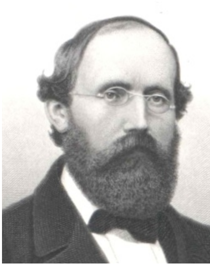
European Research Council
Established by the European Commission

FernUni.ch
UniDistance.ch

Riemann's zeta-function

- Zeta-function:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \qquad \begin{pmatrix} s \in \mathbb{C}, \\ \mathrm{Re}(s) > 1 \end{pmatrix}$$



FernUni.ch
UniDistance.ch

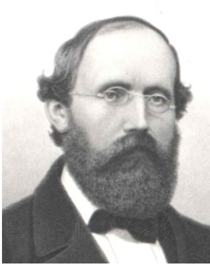
Riemann's zeta-function

- Zeta-function:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \qquad \left(\begin{array}{c} s \in \mathbb{C}, \\ \mathrm{Re}(s) > 1 \end{array} \right)$$

- Euler's product formula:

$$\zeta(s) = \prod_{p \text{ prime}} \left(\frac{1}{1 - p^{-s}} \right)$$



Riemann's zeta-function

- Zeta-function:

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \qquad \begin{pmatrix} s \in \mathbb{C}, \\ \mathrm{Re}(s) > 1 \end{pmatrix}$$

- Euler's product formula:

$$\zeta(s) = \prod_{p \text{ prime}} \left(\frac{1}{1 - p^{-s}} \right)$$

- Riemann: use this & complex analysis to study **distribution of primes**

FernUni.ch
UniDistance.ch

Number fields

- Finite field extensions of $\mathbb{Q}$, eg

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\} \qquad (d \in \mathbb{N} \text{ squarefree})$$

Number fields

- Finite field extensions of $\mathbb{Q}$, eg

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\} \qquad (d \in \mathbb{N} \text{ squarefree})$$

- $\mathcal{O}_K$ ring of **algebraic integers** in K

FernUni.ch
UniDistance.ch

Number fields

- Finite field extensions of $\mathbb{Q}$, eg

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\} \qquad (d \in \mathbb{N} \text{ squarefree})$$

- $\mathcal{O}_K$ ring of **algebraic integers** in K
- Not a UFD, but have unique factorisation of *ideals* into prime ideals

FernUni.ch
UniDistance.ch

Number fields

- Finite field extensions of $\mathbb{Q}$, eg

$$\mathbb{Q}(\sqrt{d}) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\} \qquad (d \in \mathbb{N} \text{ squarefree})$$

- $\mathcal{O}_K$ ring of **algebraic integers** in K
- Not a UFD, but have unique factorisation of *ideals* into prime ideals
- **Dedekind zeta function**:

$$\zeta_K(s) = \sum_{\mathfrak{a} \trianglelefteq \mathcal{O}_K} \frac{1}{\mathrm{Norm}(\mathfrak{a})^s} = \prod_{\substack{\mathfrak{p} \trianglelefteq \mathcal{O}_K \\ \text{prime ideal}}} (1 - \mathrm{Norm}(\mathfrak{p})^{-s})^{-1}$$

FernUni.ch
UniDistance.ch

Leading terms

Theorem (Analytic class number formula)

We have

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} R_K h_K}{w_K\sqrt{D_K}}$$

*(h_K = order of **class group**, R_K related to **units** of $\mathcal{O}_K$)*

Leading terms

Theorem (Analytic class number formula)

We have

$$\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{2^{r_1}(2\pi)^{r_2} R_K h_K}{w_K\sqrt{D_K}}$$

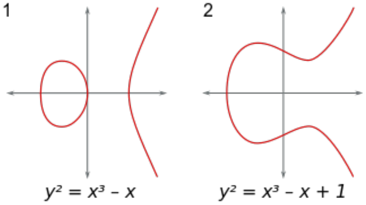
*(h_K = order of **class group**, R_K related to **units** of $\mathcal{O}_K$)*

- So the zeta-function (analytic object) *encodes* algebraic properties of K (class group / units)

FernUni.ch
UniDistance.ch

Function fields

- What other fields “behave like” algebraic number fields?

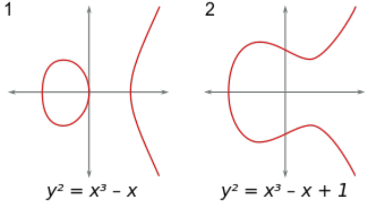


FernUni.ch
UniDistance.ch

Function fields

- What other fields "behave like" algebraic number fields?
- Answer: **Function fields** of algebraic curves over finite fields, e.g.

$$y^2 = f(x), \qquad f \in \mathbb{F}_p[X]$$



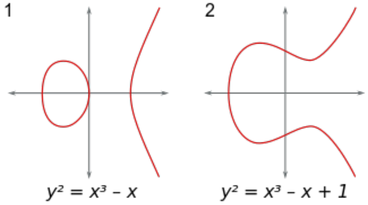
FernUni.ch
UniDistance.ch

Function fields

- What other fields "behave like" algebraic number fields?
- Answer: **Function fields** of algebraic curves over finite fields, e.g.

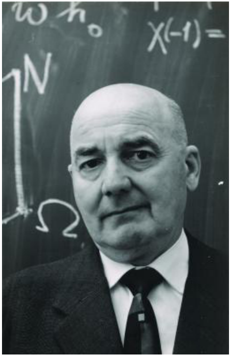
$$y^2 = f(x), \qquad f \in \mathbb{F}_p[X]$$

- Prime ideal $\mathfrak{p}$ for each point (x, y) of $\mathcal{C}$ (over $\mathbb{F}_p$ or any extension, up to Galois action)



Zeta functions of curves

- Can form a **zeta function** of $\mathcal{C}$:
  $\zeta_{\mathcal{C}}(s) = \prod_{\mathfrak{p}}(1 - \mathrm{Norm}(\mathfrak{p})^{-s})^{-1}$

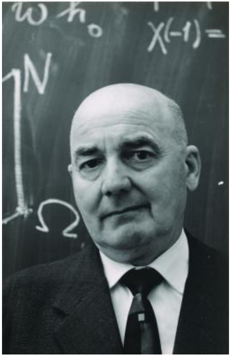


FernUni.ch
UniDistance.ch

Zeta functions of curves

- Can form a **zeta function** of $\mathcal{C}$: $\zeta_{\mathcal{C}}(s) = \prod_{\mathfrak{p}}(1 - \mathrm{Norm}(\mathfrak{p})^{-s})^{-1}$
- "Generating function" for points on $\mathcal{C}$:

$$\zeta_{\mathcal{C}}(s) = \exp\left(\sum_{k \geq 1} \frac{\#\mathcal{C}(\mathbb{F}_{p^n})}{n} p^{-ns}\right)$$



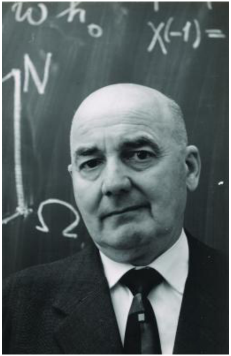
FernUni.ch
UniDistance.ch

Zeta functions of curves

- Can form a **zeta function** of $\mathcal{C}$: $\zeta_{\mathcal{C}}(s) = \prod_{\mathfrak{p}}(1 - \mathrm{Norm}(\mathfrak{p})^{-s})^{-1}$
- "Generating function" for points on $\mathcal{C}$:

$$\zeta_{\mathcal{C}}(s) = \exp\left(\sum_{k\geq 1} \frac{\#\mathcal{C}(\mathbb{F}_{p^n})}{n} p^{-ns}\right)$$

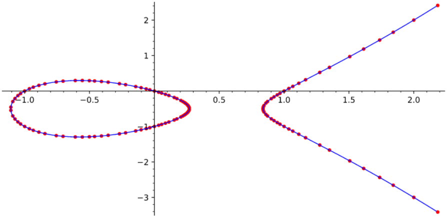
- Hasse, Weil: this is a *rational function* of p^{-s}, and satisfies an analogue of the Riemann hypothesis.



FernUni.ch
UniDistance.ch

Back to the rational numbers

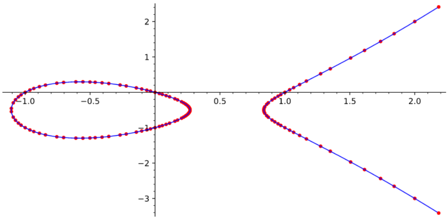
- What about algebraic curves over $\mathbb{Q}$ (or other number fields)?



FernUni.ch
UniDistance.ch

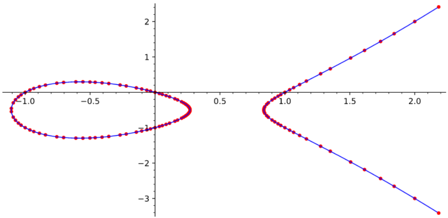
Back to the rational numbers

- What about algebraic curves over $\mathbb{Q}$ (or other number fields)?
- First interesting case: *elliptic* curves, $y^2 =$ cubic in x



Back to the rational numbers

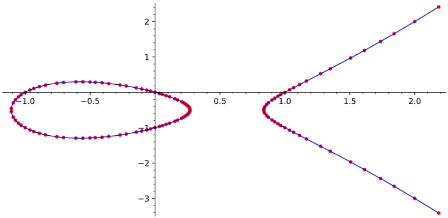
- What about algebraic curves over $\mathbb{Q}$ (or other number fields)?
- First interesting case: *elliptic* curves, $y^2 = \text{cubic in } x$
- Set of rational points can be finite, or infinite



FernUni.ch
UniDistance.ch

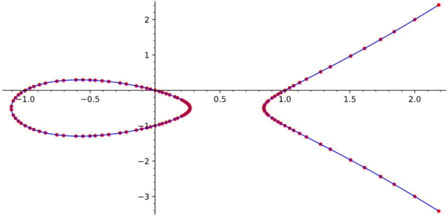
Back to the rational numbers

- What about algebraic curves over $\mathbb{Q}$ (or other number fields)?
- First interesting case: *elliptic* curves, $y^2 =$ cubic in x
- Set of rational points can be finite, or infinite
- Can show it has an *abelian group* structure; but what is its **rank**?



Back to the rational numbers

- What about algebraic curves over $\mathbb{Q}$ (or other number fields)?
- First interesting case: *elliptic* curves, $y^2 =$ cubic in x
- Set of rational points can be finite, or infinite
- Can show it has an *abelian group* structure; but what is its **rank**?
- Maybe some sort of generating function might explain this?



An outrageous idea

- Can reduce equations mod p (excluding finitely many bad primes)

$$E \rightsquigarrow E_p \quad \text{curve} / \mathbb{F}_p$$

FernUni.ch
UniDistance.ch

An outrageous idea

- Can reduce equations mod p (excluding finitely many bad primes)

$$E \rightsquigarrow E_p \quad \text{curve } / \ \mathbb{F}_p$$

- Maybe if E has “lots” of points over $\mathbb{Q}$, it should also have more than expected number of points over $\mathbb{F}_p$ (for lots of primes p)

FernUni.ch
UniDistance.ch

An outrageous idea

- Can reduce equations mod p (excluding finitely many bad primes)

$$E \rightsquigarrow E_p \quad \text{curve} / \mathbb{F}_p$$

- Maybe if E has "lots" of points over $\mathbb{Q}$, it should also have more than expected number of points over $\mathbb{F}_p$ (for lots of primes p)
- **Outrageous idea**: just smash the $\zeta_{E_p}(s)$ for different p together into an infinite product

FernUni.ch
UniDistance.ch

An outrageous idea

- Can reduce equations mod p (excluding finitely many bad primes)

$$E \rightsquigarrow E_p \quad \text{curve} / \mathbb{F}_p$$

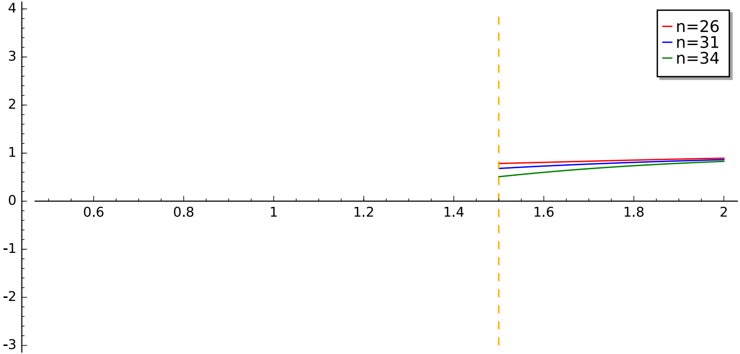
- Maybe if E has “lots” of points over $\mathbb{Q}$, it should also have more than expected number of points over $\mathbb{F}_p$ (for lots of primes p)
- **Outrageous idea**: just smash the $\zeta_{E_p}(s)$ for different p together into an infinite product
- Slight refinement:

$$L(E, s) := \frac{\zeta(s)\zeta(s-1)}{\prod_p \zeta_{E_p}(s)} \qquad \text{(removes some junk terms)}$$

FernUni.ch
UniDistance.ch

Some examples

$$\boxed{L(E, s) \text{ for } E := Y^2 = X^3 - n^2 X}$$

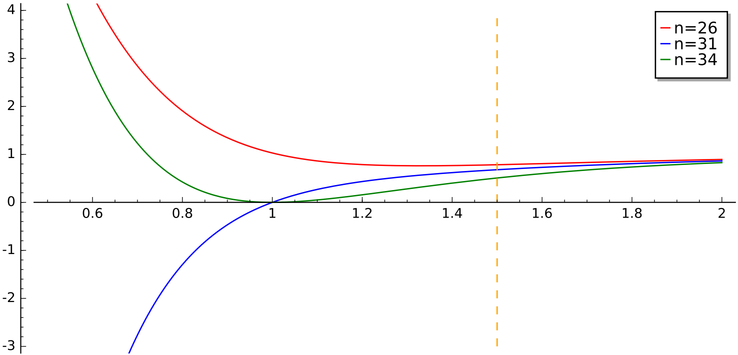


Rank of $E(\mathbb{Q})$: 0, 1, 2 respectively

FernUni.ch
UniDistance.ch

Analytic continuation

$$\boxed{L(E,s) \text{ for } E := Y^2 = X^3 - n^2 X}$$



Rank of $E(\mathbb{Q})$: 0, 1, 2 respectively

The Birch–Swinnerton-Dyer conjecture

Conjecture (Birch–Swinnerton-Dyer, 1963)

Let E be an elliptic curve. Then: $\operatorname{ord}_{s=1} L(E, s) = \underbrace{r(E)}_{\text{rank of } E(\mathbb{Q})}$.

FernUni.ch
UniDistance.ch

The Birch–Swinnerton-Dyer conjecture

Conjecture (Birch–Swinnerton-Dyer, 1963)

Let E be an elliptic curve. Then: $\operatorname{ord}_{s=1} L(E,s) = \underbrace{r(E)}_{\text{rank of } E(\mathbb{Q})}$.

- Also predict **leading term** at $s = 1$ in terms of finer algebraic invariants (regulator, Shafarevich–Tate group)

FernUni.ch
UniDistance.ch

Generalising the BSD conjecture

- Definition of L-function makes sense much more generally:

Generalising the BSD conjecture

- Definition of L-function makes sense much more generally:
  - Algebraic varieties (systems of algebraic equations, any number of variables)

FernUni.ch
UniDistance.ch

Generalising the BSD conjecture

- Definition of L-function makes sense much more generally:
  - Algebraic varieties (systems of algebraic equations, any number of variables)
  - Varieties over any number field (not just $\mathbb{Q}$)

FernUni.ch
UniDistance.ch

Generalising the BSD conjecture

- Definition of L-function makes sense much more generally:
  - Algebraic varieties (systems of algebraic equations, any number of variables)
  - Varieties over any number field (not just $\mathbb{Q}$)
  - *motives* = "pieces" of the geometry of algebraic varieties

FernUni.ch
UniDistance.ch

Generalising the BSD conjecture

- Definition of L-function makes sense much more generally:
  - Algebraic varieties (systems of algebraic equations, any number of variables)
  - Varieties over any number field (not just $\mathbb{Q}$)
  - *motives* = "pieces" of the geometry of algebraic varieties
- Always given by infinite products over primes (Euler products)

FernUni.ch
UniDistance.ch

Generalising the BSD conjecture

- Definition of *L*-function makes sense much more generally:
  - Algebraic varieties (systems of algebraic equations, any number of variables)
  - Varieties over any number field (not just $\mathbb{Q}$)
  - *motives* = "pieces" of the geometry of algebraic varieties
- Always given by infinite products over primes (Euler products)
- Less obvious how to generalise *rank*

Generalising the BSD conjecture

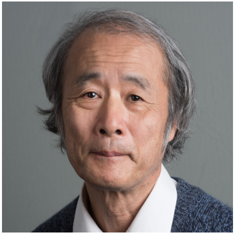
- Definition of L-function makes sense much more generally:
  - Algebraic varieties (systems of algebraic equations, any number of variables)
  - Varieties over any number field (not just $\mathbb{Q}$)
  - *motives* = "pieces" of the geometry of algebraic varieties
- Always given by infinite products over primes (Euler products)
- Less obvious how to generalise *rank*
  - Works for varieties when the points have a group structure (Abelian varieties)

FernUni.ch
UniDistance.ch

Generalising the BSD conjecture

- Definition of *L*-function makes sense much more generally:
  - Algebraic varieties (systems of algebraic equations, any number of variables)
  - Varieties over any number field (not just $\mathbb{Q}$)
  - *motives* = "pieces" of the geometry of algebraic varieties
- Always given by infinite products over primes (Euler products)
- Less obvious how to generalise *rank*
  - Works for varieties when the points have a group structure (Abelian varieties)
  - Doesn't make sense for general motives

The Bloch–Kato conjecture

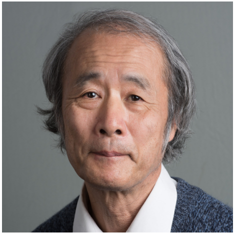


Conjecture (Bloch–Kato, 1990)

For any motive M and $n \in \mathbb{Z}$, we have

$$\operatorname{ord}_{s=n} L(M, s) \ =$$

The Bloch–Kato conjecture

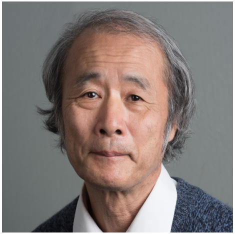


Conjecture (Bloch–Kato, 1990)

For any motive M and $n \in \mathbb{Z}$, we have

$$\operatorname{ord}_{s=n} L(M, s) \;=$$

The Bloch–Kato conjecture



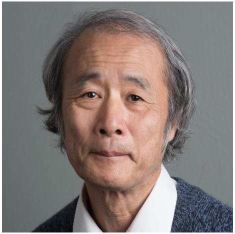
Conjecture (Bloch–Kato, 1990)

For any motive M and $n \in \mathbb{Z}$, we have

$$\mathrm{ord}_{s=n} L(M, s) = \text{rank of certain } \textbf{cohomology group} \text{ (Selmer group) attached to } M \text{ and } n$$

FernUni.ch
UniDistance.ch

The Bloch–Kato conjecture



Conjecture (Bloch–Kato, 1990)

For any motive M and $n \in \mathbb{Z}$, we have

$$\operatorname{ord}_{s=n} L(M, s) = \textit{rank of certain } \textbf{\textit{cohomology group}} \\ \textit{(Selmer group) attached to } M \textit{ and } n$$

- Refined form predicting leading term

FernUni.ch
UniDistance.ch

FernUni.ch
UniDistance.ch

BSD for small orders of vanishing

Theorem (Kolyvagin, 1989)

Let $E/\mathbb{Q}$ be an elliptic curve. If $\operatorname{ord}_{s=1} L(E,s) = 0$ or 1, then $\operatorname{rank} E(\mathbb{Q}) = \operatorname{ord}_{s=1} L(E,s)$.

BSD for small orders of vanishing

Theorem (Kolyvagin, 1989)

Let $E/\mathbb{Q}$ be an elliptic curve. If $\operatorname{ord}_{s=1} L(E,s) = 0$ or 1, then $\operatorname{rank} E(\mathbb{Q}) = \operatorname{ord}_{s=1} L(E,s)$.

- Steady progress towards leading term formula under these hypotheses (most cases done, but not all)

BSD for small orders of vanishing

Theorem (Kolyvagin, 1989)

Let $E/\mathbb{Q}$ be an elliptic curve. If $\operatorname{ord}_{s=1} L(E,s) = 0$ or 1, then $\operatorname{rank} E(\mathbb{Q}) = \operatorname{ord}_{s=1} L(E,s)$.

- Steady progress towards leading term formula under these hypotheses (most cases done, but not all)
- Originally needed to assume E **modular** – now a theorem that this always holds (Wiles, Breuil–Conrad–Diamond–Taylor)

FernUni.ch
UniDistance.ch

BSD for small orders of vanishing

Theorem (Kolyvagin, 1989)

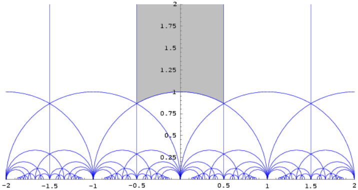
Let $E/\mathbb{Q}$ be an elliptic curve. If $\operatorname{ord}_{s=1} L(E, s) = 0$ *or* 1*, then* $\operatorname{rank} E(\mathbb{Q}) = \operatorname{ord}_{s=1} L(E, s)$*.*

- Steady progress towards leading term formula under these hypotheses (most cases done, but not all)
- Originally needed to assume E **modular** – now a theorem that this always holds (Wiles, Breuil–Conrad–Diamond–Taylor)
- Still know virtually nothing for order of vanishing ≥ 2

FernUni.ch
UniDistance.ch

Modularity

- Upper half-plane $\mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$



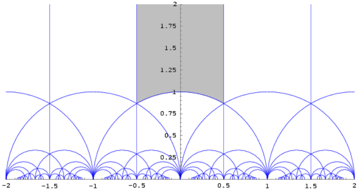
FernUni.ch
UniDistance.ch

Modularity

- Upper half-plane $\mathbb{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$
- For $N \geq 1$ the group

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ Nc & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}, ad - Nbc = 1 \right\}$$

acts on $\mathbb{H}$, and on compactification $\mathbb{H}^* = \mathbb{H} \cup \mathbb{P}^1(\mathbb{Q})$

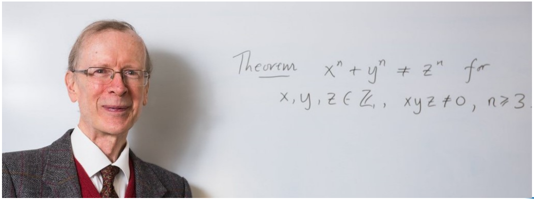


FernUni.ch
UniDistance.ch

Modularity

- Say E is *modular* if for some N, $\exists$ complex-analytic map

$$\phi : \Gamma_0(N)\backslash\mathbb{H}^* \twoheadrightarrow E(\mathbb{C}).$$



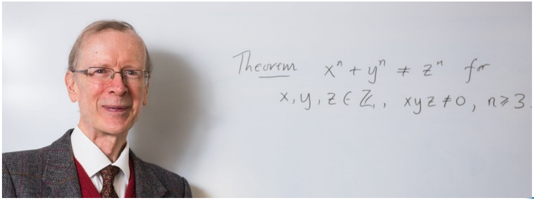
FernUni.ch
UniDistance.ch

Modularity

- Say E is *modular* if for some N, $\exists$ complex-analytic map

$$\phi : \Gamma_0(N)\backslash\mathbb{H}^* \twoheadrightarrow E(\mathbb{C}).$$

- **Taniyama–Shimura conjecture**: all $E/\mathbb{Q}$ are modular (proved by Taylor–Wiles, Breuil–Conrad–Diamond–Taylor)

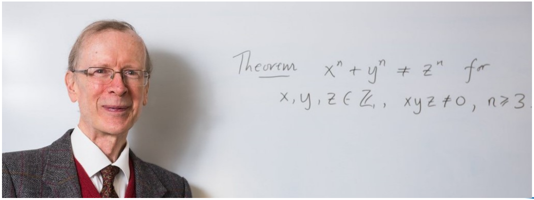


Modularity

- Say E is *modular* if for some N, $\exists$ complex-analytic map

$$\phi : \Gamma_0(N)\backslash\mathbb{H}^* \twoheadrightarrow E(\mathbb{C}).$$

- **Taniyama–Shimura conjecture**: all $E/\mathbb{Q}$ are modular (proved by Taylor–Wiles, Breuil–Conrad–Diamond–Taylor)
- Key to proof of Fermat's last theorem



FernUni.ch
UniDistance.ch

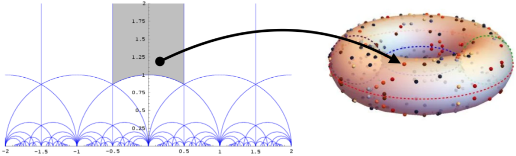
CM points and Heegner points

- A **CM point** is a point in $\mathbb{H}$ of form $a+\sqrt{-d}$, $a, d \in \mathbb{Q}$, $d > 0$

FernUni.ch
UniDistance.ch

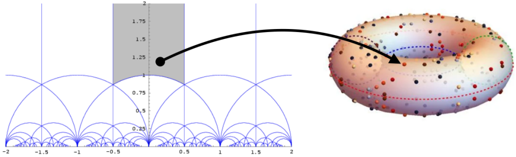
CM points and Heegner points

- A **CM point** is a point in $\mathbb{H}$ of form $a + \sqrt{-d}$, $a, d \in \mathbb{Q}$, $d > 0$
- **Heegner point** on a modular elliptic curve: image of a CM point under $\phi : \Gamma_0(N)\backslash\mathbb{H}^* \twoheadrightarrow E(\mathbb{C})$



CM points and Heegner points

- A **CM point** is a point in $\mathbb{H}$ of form $a + \sqrt{-d}$, $a, d \in \mathbb{Q}$, $d > 0$
- **Heegner point** on a modular elliptic curve: image of a CM point under $\phi : \Gamma_0(N)\backslash\mathbb{H}^* \twoheadrightarrow E(\mathbb{C})$

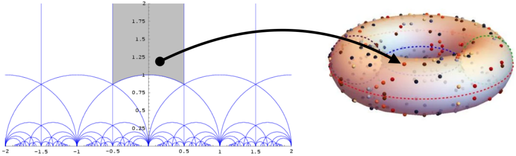


- Miracle: Heegner points are *algebraic*, i.e. lie in $E(\overline{\mathbb{Q}})$ (entirely un-obvious from construction)

FernUni.ch
UniDistance.ch

CM points and Heegner points

- A **CM point** is a point in $\mathbb{H}$ of form $a + \sqrt{-d}$, $a, d \in \mathbb{Q}$, $d > 0$
- **Heegner point** on a modular elliptic curve: image of a CM point under $\phi : \Gamma_0(N)\backslash\mathbb{H}^* \twoheadrightarrow E(\mathbb{C})$



- Miracle: Heegner points are *algebraic*, i.e. lie in $E(\overline{\mathbb{Q}})$ (entirely un-obvious from construction)
- *Shimura reciprocity* describes precisely which number field each one lives in (always an abelian extension of $\mathbb{Q}(\sqrt{-d})$)

FernUni.ch
UniDistance.ch

Kolyvagin's Euler system

- Heegner theory gives points $c_n \in E(K_n)$ for an infinite family of number fields K_n

FernUni.ch
UniDistance.ch

Kolyvagin's Euler system

- Heegner theory gives points $c_n \in E(K_n)$ for an infinite family of number fields K_n
- Norm-compatibility relation: for $n \mid m$, have $K_n \subseteq K_m$ and

$$\mathrm{norm}_{K_n}^{K_m}(c_m) = \Big(\prod_{\substack{p \mid m \\ p \nmid n}} P_p\Big) \cdot c_n,$$

where P_p = factor at p in Euler product for L-series

FernUni.ch
UniDistance.ch

Kolyvagin's Euler system

- Heegner theory gives points $c_n \in E(K_n)$ for an infinite family of number fields K_n
- Norm-compatibility relation: for $n \mid m$, have $K_n \subseteq K_m$ and

$$\mathrm{norm}_{K_n}^{K_m}(c_m) = \Big(\prod_{\substack{p \mid m \\ p \nmid n}} P_p\Big) \cdot c_n,$$

  where P_p = factor at p in Euler product for L-series
- **Gross–Zagier theorem**: bottom point c_1 is non-trivial if $\mathrm{ord}_{s=1} L(E, s) \leq 1$

Kolyvagin's Euler system

- Heegner theory gives points $c_n \in E(K_n)$ for an infinite family of number fields K_n
- Norm-compatibility relation: for $n \mid m$, have $K_n \subseteq K_m$ and

$$\mathrm{norm}_{K_n}^{K_m}(c_m) = \Big(\prod_{\substack{p \mid m \\ p \nmid n}} P_p\Big) \cdot c_n,$$

  where $P_p =$ factor at p in Euler product for L-series
- **Gross–Zagier theorem**: bottom point c_1 is non-trivial if $\mathrm{ord}_{s=1} L(E, s) \leq 1$
- Delicate manipulations with duality theory of Galois cohomology $\Rightarrow$ bounds on $E(\mathbb{Q})$: either it's zero, or c_1 generates it up to a finite error.

FernUni.ch
UniDistance.ch

Beyond elliptic curves

- Are there Euler systems for other L-functions / motives?

Beyond elliptic curves

- Are there Euler systems for other L-functions / motives?
  - Rubin, Kato, Perrin-Riou: general *definition* of what Euler systems should be

Beyond elliptic curves

- Are there Euler systems for other L-functions / motives?
  - Rubin, Kato, Perrin-Riou: general *definition* of what Euler systems should be
  - when these exist, get bounds on Selmer groups ($\rightsquigarrow$ Bloch–Kato?)

FernUni.ch
UniDistance.ch

Beyond elliptic curves

- Are there Euler systems for other L-functions / motives?
  - Rubin, Kato, Perrin-Riou: general *definition* of what Euler systems should be
  - when these exist, get bounds on Selmer groups ($\rightsquigarrow$ Bloch–Kato?)
- Besides Kolyvagin, two “easy” examples from units in number fields (cyclotomic / elliptic units)

Beyond elliptic curves

- Are there Euler systems for other L-functions / motives?
  - Rubin, Kato, Perrin-Riou: general *definition* of what Euler systems should be
  - when these exist, get bounds on Selmer groups ($\rightsquigarrow$ Bloch–Kato?)
- Besides Kolyvagin, two "easy" examples from units in number fields (cyclotomic / elliptic units)
- Wiles: unsuccessful attempt to build Euler system for Sym^2 of elliptic curve

Beyond elliptic curves

- Are there Euler systems for other L-functions / motives?
  - Rubin, Kato, Perrin-Riou: general *definition* of what Euler systems should be
  - when these exist, get bounds on Selmer groups ($\rightsquigarrow$ Bloch–Kato?)
- Besides Kolyvagin, two “easy” examples from units in number fields (cyclotomic / elliptic units)
- Wiles: unsuccessful attempt to build Euler system for Sym^2 of elliptic curve
- Kato (2004): Euler system for a modular form

FernUni.ch
UniDistance.ch

Beyond elliptic curves

- Are there Euler systems for other L-functions / motives?
  - Rubin, Kato, Perrin-Riou: general *definition* of what Euler systems should be
  - when these exist, get bounds on Selmer groups ($\rightsquigarrow$ Bloch–Kato?)
- Besides Kolyvagin, two “easy” examples from units in number fields (cyclotomic / elliptic units)
- Wiles: unsuccessful attempt to build Euler system for Sym^2 of elliptic curve
- Kato (2004): Euler system for a modular form
- No more examples for > 10 years

FernUni.ch
UniDistance.ch

Beilinson–Flach elements

Theorem (Lei–L.–Zerbes 2014, Kings–L.–Zerbes 2017)

There is a non-trivial Euler system attached to the Rankin–Selberg convolution of two modular forms.

Beilinson–Flach elements

Theorem (Lei–L.–Zerbes 2014, Kings–L.–Zerbes 2017)

There is a non-trivial Euler system attached to the Rankin–Selberg convolution of two modular forms.

- Builds on work of Beilinson, Flach, and Bertolini–Darmon–Rotger

FernUni.ch
UniDistance.ch

Beilinson–Flach elements

Theorem (Lei–L.–Zerbes 2014, Kings–L.–Zerbes 2017)

There is a non-trivial Euler system attached to the Rankin–Selberg convolution of two modular forms.

- Builds on work of Beilinson, Flach, and Bertolini–Darmon–Rotger
- Gives new results towards Bloch–Kato, and BSD over number fields

FernUni.ch
UniDistance.ch

A production line of Euler systems

- Techniques adapted to define many new Euler systems

FernUni.ch
UniDistance.ch

A production line of Euler systems

- Techniques adapted to define many new Euler systems
- Correspond to **automorphic forms** for various matrix groups G

FernUni.ch
UniDistance.ch

A production line of Euler systems

- Techniques adapted to define many new Euler systems
- Correspond to **automorphic forms** for various matrix groups G
  - $\mathrm{GL}_2 \times \mathrm{GL}_2$ (Rankin–Selberg)

FernUni.ch
UniDistance.ch

A production line of Euler systems

- Techniques adapted to define many new Euler systems
- Correspond to **automorphic forms** for various matrix groups G
  - $\mathrm{GL}_2 \times \mathrm{GL}_2$ (Rankin–Selberg)
  - GSp_4 (Siegel modular forms)

FernUni.ch
UniDistance.ch

A production line of Euler systems

- Techniques adapted to define many new Euler systems
- Correspond to **automorphic forms** for various matrix groups G
  - $\mathrm{GL}_2 \times \mathrm{GL}_2$ (Rankin–Selberg)
  - GSp_4 (Siegel modular forms)
  - unitary groups, Hilbert modular groups, ...

FernUni.ch
UniDistance.ch

A production line of Euler systems

- Techniques adapted to define many new Euler systems
- Correspond to **automorphic forms** for various matrix groups G
  - $\mathrm{GL}_2 \times \mathrm{GL}_2$ (Rankin–Selberg)
  - GSp_4 (Siegel modular forms)
  - unitary groups, Hilbert modular groups, ...
- Uses geometry of **Shimura varieties** (generalisations of $\Gamma_0(N)\backslash\mathbb{H}$)

FernUni.ch
UniDistance.ch

A production line of Euler systems

- Techniques adapted to define many new Euler systems
- Correspond to **automorphic forms** for various matrix groups G
  - $\mathrm{GL}_2 \times \mathrm{GL}_2$ (Rankin–Selberg)
  - GSp_4 (Siegel modular forms)
  - unitary groups, Hilbert modular groups, ...
- Uses geometry of **Shimura varieties** (generalisations of $\Gamma_0(N)\backslash\mathbb{H}$)
- Proving non-triviality is more difficult (needs *explicit reciprocity laws*) – done for GSp_4, and for quadratic Hilbert modular groups

  [various works of Grossi, Lei, L., Pilloni, Skinner, Zerbes]

FernUni.ch
UniDistance.ch

Applications

1. Bloch–Kato non-zero values of L-functions of **Siegel modular forms** (for GSp_4, weight ≥ 3)

Applications

1. Bloch–Kato non-zero values of L-functions of **Siegel modular forms** (for GSp_4, weight ≥ 3)

2. BSD for **abelian surfaces** A with $L(A, 1) \neq 0$ (conditional on 2 big conjectures)

FernUni.ch
UniDistance.ch

Applications

1. Bloch–Kato non-zero values of L-functions of **Siegel modular forms** (for GSp_4, weight ≥ 3)
2. BSD for **abelian surfaces** A with $L(A, 1) \neq 0$ (conditional on 2 big conjectures)
3. Euler system for **symmetric square** of a modular form

FernUni.ch
UniDistance.ch

Applications

1. Bloch–Kato non-zero values of L-functions of **Siegel modular forms** (for GSp_4, weight ≥ 3)
2. BSD for **abelian surfaces** A with $L(A, 1) \neq 0$ (conditional on 2 big conjectures)
3. Euler system for **symmetric square** of a modular form
   - New approach to (parts of) proof of Fermat's last theorem

FernUni.ch
UniDistance.ch

Applications

1. Bloch–Kato non-zero values of L-functions of **Siegel modular forms** (for GSp_4, weight ≥ 3)
2. BSD for **abelian surfaces** A with $L(A, 1) \neq 0$ (conditional on 2 big conjectures)
3. Euler system for **symmetric square** of a modular form
   - New approach to (parts of) proof of Fermat's last theorem
   - Iwasawa main conjecture for Sym^2

FernUni.ch
UniDistance.ch

Applications

1. Bloch–Kato non-zero values of L-functions of **Siegel modular forms** (for GSp_4, weight ≥ 3)

2. BSD for **abelian surfaces** A with $L(A, 1) \neq 0$ (conditional on 2 big conjectures)

3. Euler system for **symmetric square** of a modular form
   - New approach to (parts of) proof of Fermat's last theorem
   - Iwasawa main conjecture for Sym^2
   - Cf. parallel work of Sangiovanni–Skinner

FernUni.ch
UniDistance.ch

How far can this go?

- To build Euler systems for automorphic forms on G, need two ingredients:

How far can this go?

- To build Euler systems for automorphic forms on G, need two ingredients:
  - Subgroup H sitting "nicely" inside G

FernUni.ch
UniDistance.ch

How far can this go?

- To build Euler systems for automorphic forms on G, need two ingredients:
  - Subgroup H sitting “nicely” inside G
  - Family of cohomology classes for the Shimura variety of H

FernUni.ch
UniDistance.ch

How far can this go?

- To build Euler systems for automorphic forms on G, need two ingredients:
  - Subgroup H sitting "nicely" inside G
  - Family of cohomology classes for the Shimura variety of H
- Second ingredient can be **identity class** $1_H \in H^0(\mathrm{Sh}_H)$

How far can this go?

- To build Euler systems for automorphic forms on G, need two ingredients:
  - Subgroup H sitting "nicely" inside G
  - Family of cohomology classes for the Shimura variety of H
- Second ingredient can be **identity class** $1_H \in H^0(\mathrm{Sh}_H)$
  - Not a trivial case!

How far can this go?

- To build Euler systems for automorphic forms on G, need two ingredients:
  - Subgroup H sitting “nicely” inside G
  - Family of cohomology classes for the Shimura variety of H
- Second ingredient can be **identity class** $1_H \in H^0(\mathrm{Sh}_H)$
  - Not a trivial case!
  - Covers Kolyvagin’s Heegner points ($G = \mathrm{GL}_2, H = U(1)$) and other “anticyclotomic” Euler systems

FernUni.ch
UniDistance.ch

How far can this go?

- To build Euler systems for automorphic forms on G, need two ingredients:
  - Subgroup H sitting “nicely” inside G
  - Family of cohomology classes for the Shimura variety of H
- Second ingredient can be **identity class** $1_H \in H^0(\mathrm{Sh}_H)$
  - Not a trivial case!
  - Covers Kolyvagin’s Heegner points ($G = \mathrm{GL}_2, H = U(1)$) and other “anticyclotomic” Euler systems
- ... or **Siegel units** when $H =$ product of GL_2’s

FernUni.ch
UniDistance.ch

How far can this go?

- To build Euler systems for automorphic forms on G, need two ingredients:
  - Subgroup H sitting "nicely" inside G
  - Family of cohomology classes for the Shimura variety of H
- Second ingredient can be **identity class** $1_H \in H^0(\mathrm{Sh}_H)$
  - Not a trivial case!
  - Covers Kolyvagin's Heegner points ($G = \mathrm{GL}_2, H = U(1)$) and other "anticyclotomic" Euler systems
- ... or **Siegel units** when $H =$ product of GL_2's
  - Kato's ES, and all the examples on last slide

How far can this go?

- To build Euler systems for automorphic forms on G, need two ingredients:
  - Subgroup H sitting "nicely" inside G
  - Family of cohomology classes for the Shimura variety of H
- Second ingredient can be **identity class** $1_H \in H^0(\mathrm{Sh}_H)$
  - Not a trivial case!
  - Covers Kolyvagin's Heegner points ($G = \mathrm{GL}_2, H = U(1)$) and other "anticyclotomic" Euler systems
- ... or **Siegel units** when $H =$ product of GL_2's
  - Kato's ES, and all the examples on last slide
- ... or something else? [Sangiovanni–Skinner, in preparation]

FernUni.ch
UniDistance.ch

Spherical pairs

- Correct notion of ‘H sits nicely inside G’ : (G, H) should be a **spherical pair**

Spherical pairs

- Correct notion of 'H sits nicely inside G' : (G, H) should be a **spherical pair**
- Much-studied concept in representation theory

Spherical pairs

- Correct notion of 'H sits nicely inside G' : (G, H) should be a **spherical pair**
- Much-studied concept in representation theory
- Connections to number theory recently emerging (Sakellaridis–Venkatesh, Wei Zhang)

FernUni.ch
UniDistance.ch

Spherical pairs

- Correct notion of 'H sits nicely inside G' : (G, H) should be a **spherical pair**
- Much-studied concept in representation theory
- Connections to number theory recently emerging (Sakellaridis–Venkatesh, Wei Zhang)
- Gan–Gross–Prasad conjectures: $U(n) \subset U(n) \times U(n+1)$, $SO(n) \subset SO(n) \times SO(n+1)$

FernUni.ch
UniDistance.ch

Spherical pairs

- Correct notion of 'H sits nicely inside G' : (G, H) should be a **spherical pair**
- Much-studied concept in representation theory
- Connections to number theory recently emerging (Sakellaridis–Venkatesh, Wei Zhang)
- Gan–Gross–Prasad conjectures: $U(n) \subset U(n) \times U(n+1)$, $SO(n) \subset SO(n) \times SO(n+1)$
- Many more cases to explore!

FernUni.ch
UniDistance.ch