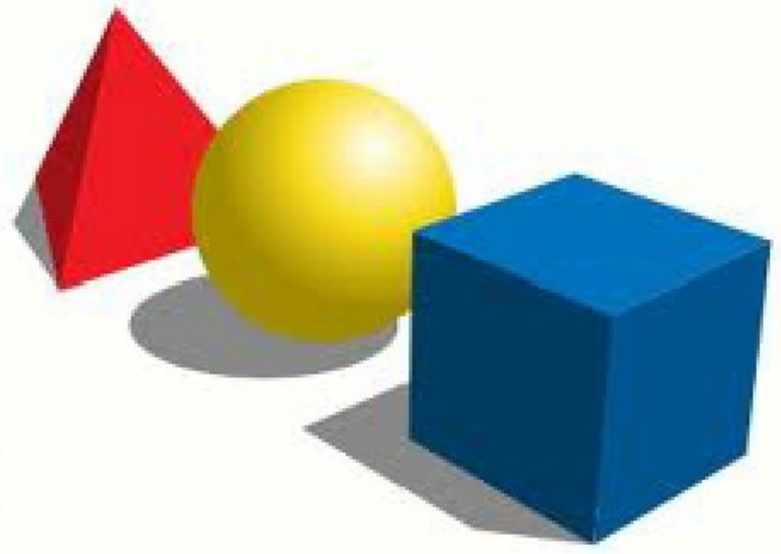
Numbers and shapes

Henri Darmon

Hugh C. Morris Lecture

Calgary, November 1, 2012



Diophantine equations

A *diophantine equation* is a system of polynomial equations, in which the variables are only allowed to take *integer values*. (One sometimes considers also *rational solutions*.)

Solutions to differential equations typically admit natural interpretations in terms of systems (arising in physics, biology, finance, ...) which one is trying to model.

Is something similar true for diophantine equations?

Question: What makes a diophantine equation interesting?

Diophantine equations

A *diophantine equation* is a system of polynomial equations, in which the variables are only allowed to take *integer values*. (One sometimes considers also *rational solutions*.)

Solutions to differential equations typically admit natural interpretations in terms of systems (arising in physics, biology, finance, ...) which one is trying to model.

Is something similar true for diophantine equations?

Question: What makes a diophantine equation interesting?

Diophantine equations

A *diophantine equation* is a system of polynomial equations, in which the variables are only allowed to take *integer values*. (One sometimes considers also *rational solutions*.)

Solutions to differential equations typically admit natural interpretations in terms of systems (arising in physics, biology, finance, . . .) which one is trying to model.

Is something similar true for diophantine equations?

Question: What makes a diophantine equation interesting?

Diophantine equations

A *diophantine equation* is a system of polynomial equations, in which the variables are only allowed to take *integer values*. (One sometimes considers also *rational solutions*.)

Solutions to differential equations typically admit natural interpretations in terms of systems (arising in physics, biology, finance, ...) which one is trying to model.

Is something similar true for diophantine equations?

Question: What makes a diophantine equation interesting?

Diophantine equations

A *diophantine equation* is a system of polynomial equations, in which the variables are only allowed to take *integer values*. (One sometimes considers also *rational solutions*.)

Solutions to differential equations typically admit natural interpretations in terms of systems (arising in physics, biology, finance, ...) which one is trying to model.

Is something similar true for diophantine equations?

Question: What makes a diophantine equation interesting?

An equation at random

Is the equation

$$x^{1297}y^{31} - 11 \cdot y^{72}z^{10} + 137 \cdot xyzw^{13} - 67 \cdot x^{17}y^{7}z^{8}w^{3}$$
$$+3572398754 \cdot x^{2}y^{3}z^{4}w^{101} + w^{15} + 3746 \cdot xyzw = 0$$

interesting?

Probably not.

An equation at random

Is the equation

$$x^{1297}y^{31} - 11 \cdot y^{72}z^{10} + 137 \cdot xyzw^{13} - 67 \cdot x^{17}y^{7}z^{8}w^{3}$$
$$+3572398754 \cdot x^{2}y^{3}z^{4}w^{101} + w^{15} + 3746 \cdot xyzw = 0$$

interesting?

Probably not.

Fermat's Last Theorem

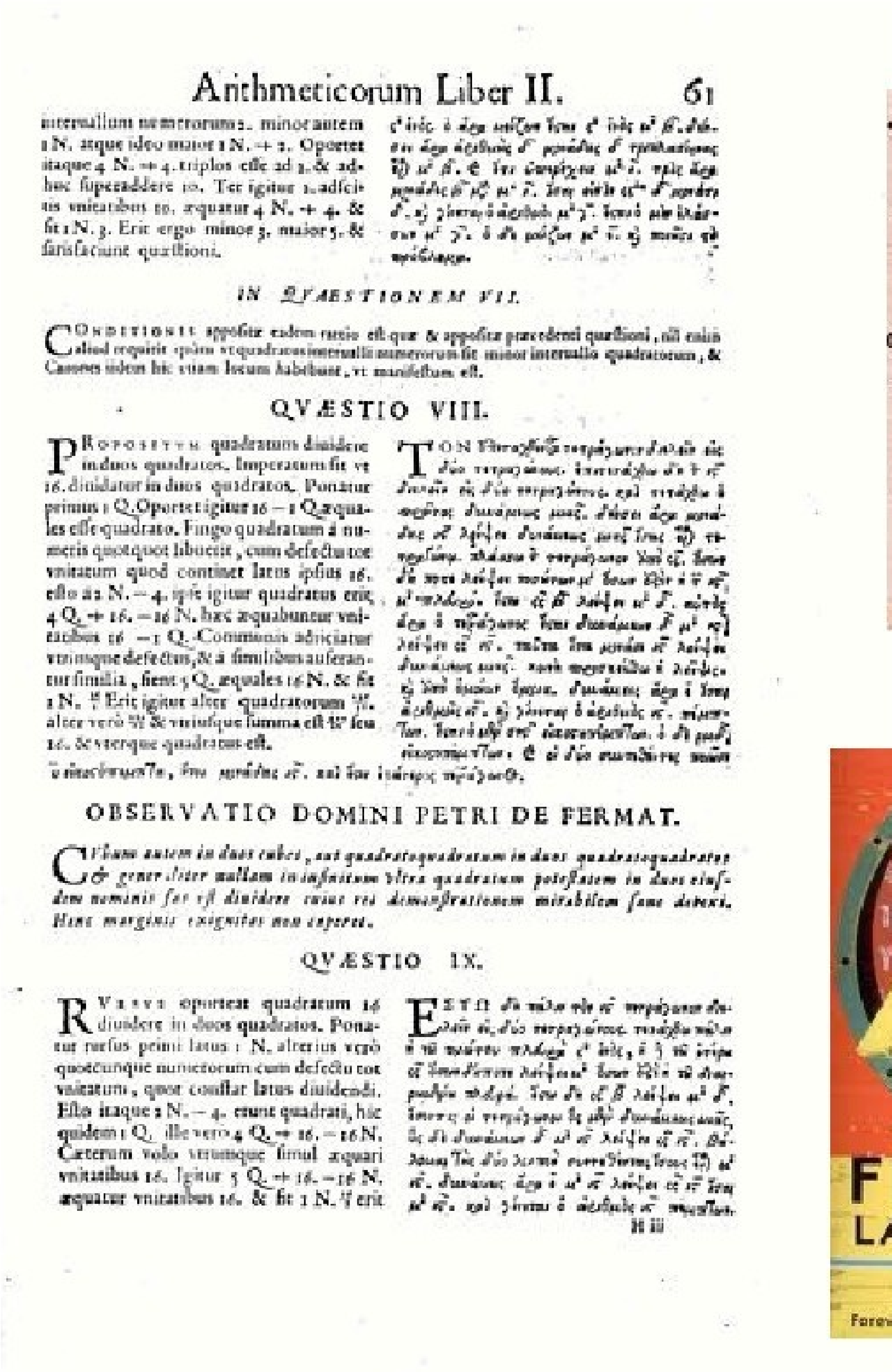
Theorem (Wiles)

If $n \geq 3$, the equation

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

has no solutions $(x, y, z) \in \mathbb{Z}^3$ with $xyz \neq 0$.

This equation is certainly interesting!



Arithmeticorum Liber II. 61

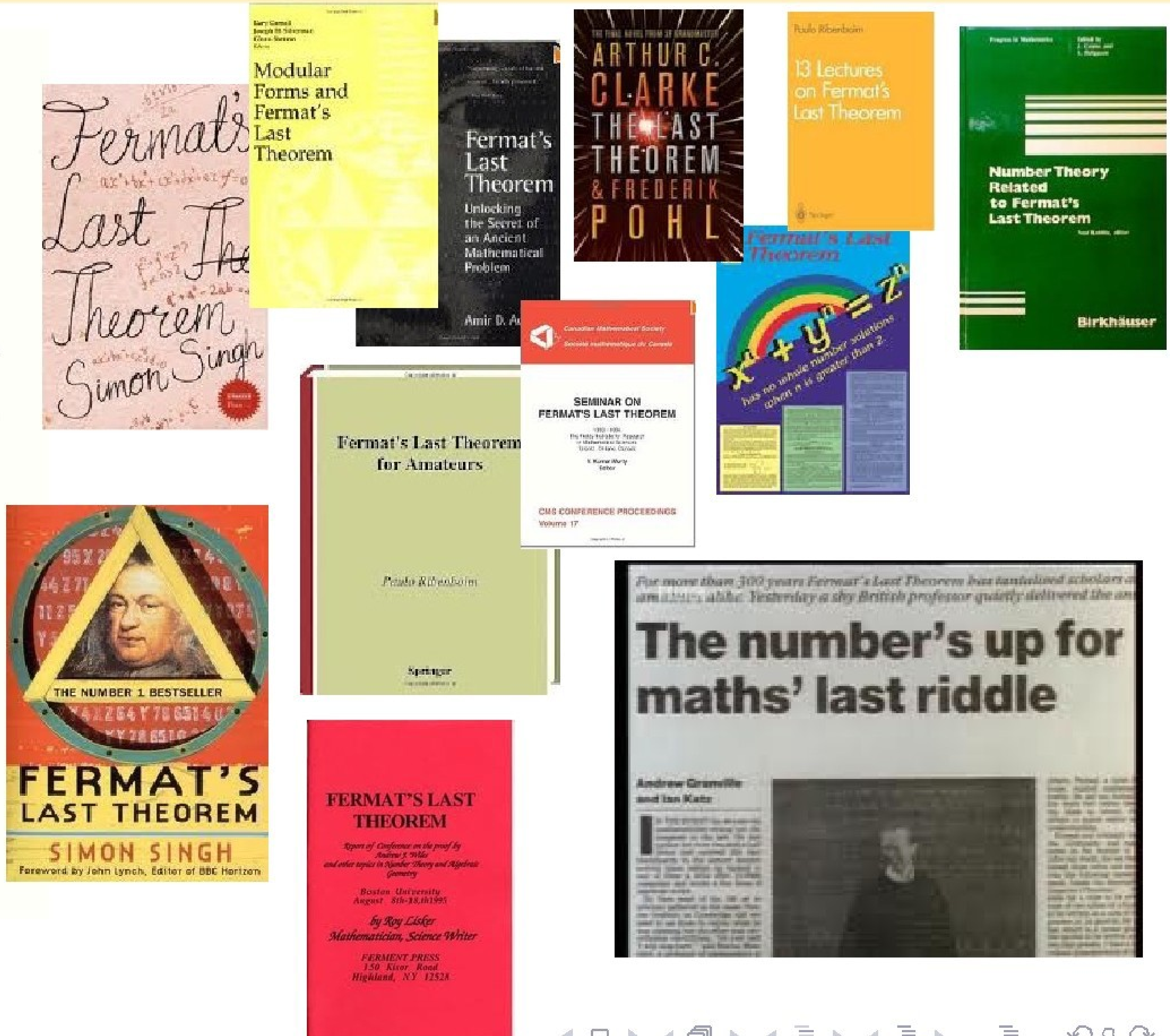
IN QVAESTIONEM VII.

QVAESTIO VIII.

OBSERVATIO DOMINI PETRI DE FERMAT.

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est diuidere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

QVAESTIO IX.



Frey's equation

A putative solution $a^p + b^p = c^p$ to the Fermat equation gives rise to the *auxiliary equation* in two variables x, y:

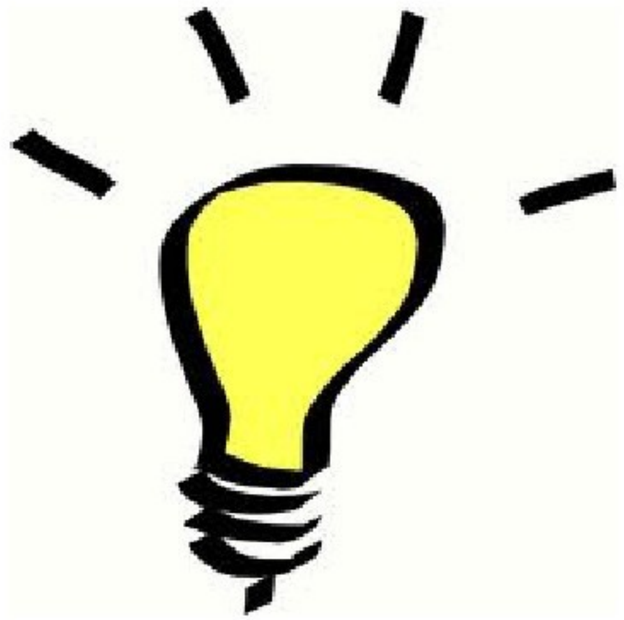
$$E_{a,b,c} : y^2 = x(x - a^p)(x + b^p).$$

One is *reduced* — in a way which will seem artificial *a priori* — to understanding certain *cubic equations in two variables* well enough to show that the one above *cannot exist*.

Frey's equation

A putative solution $a^p + b^p = c^p$ to the Fermat equation gives rise to the *auxiliary equation* in two variables x, y:

$$E_{a,b,c} : y^2 = x(x - a^p)(x + b^p).$$



One is *reduced* — in a way which will seem artificial *a priori* — to understanding certain *cubic equations in two variables* well enough to show that the one above *cannot exist*.

What is special about Frey's equation?

Give any prime ℓ, consider the *reduction* of $E_{a,b,c}$ modulo ℓ.

Proposition

Frey's elliptic curve $E_{a,b,c}$ has good reduction*–i.e., no singular points — modulo ℓ if and only if $\ell \nmid abc$.*

$\ell \nmid abc$

$\ell \mid abc$

What is special about Frey's equation?

Give any prime ℓ, consider the *reduction* of $E_{a,b,c}$ modulo ℓ.

Proposition

Frey's elliptic curve $E_{a,b,c}$ has good reduction*–i.e., no singular points — modulo ℓ if and only if $\ell \nmid abc$.*

$\ell \nmid abc$

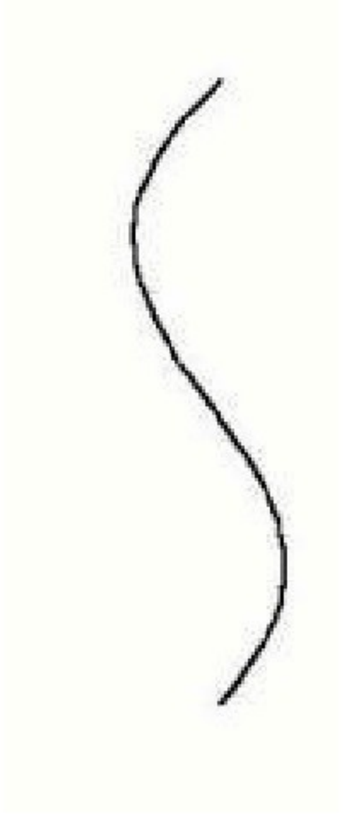
$\ell \mid abc$

What is special about Frey's equation?

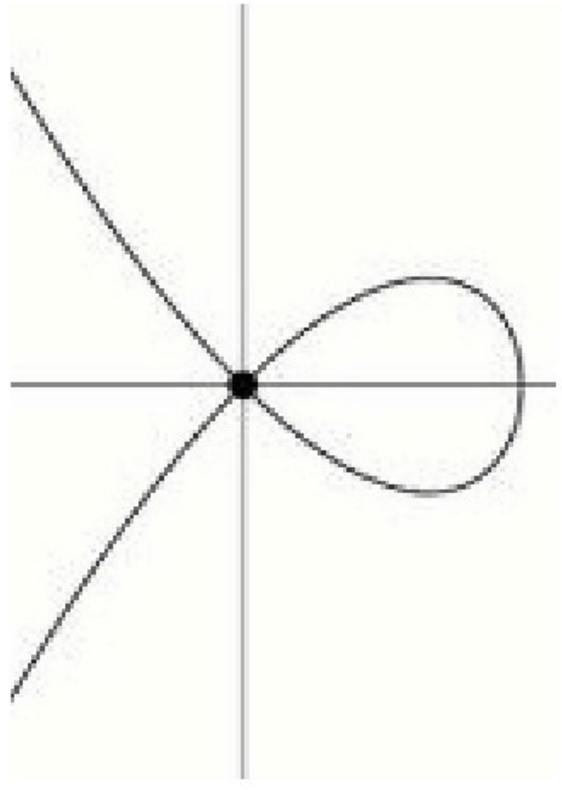
Give any prime ℓ, consider the *reduction* of $E_{a,b,c}$ modulo ℓ.

Proposition

Frey's elliptic curve $E_{a,b,c}$ has good reduction*–i.e., no singular points — modulo ℓ if and only if $\ell \nmid abc$.*



$\ell \nmid abc$



$\ell | abc$

Elliptic curves

Definition

An *elliptic curve* over $\mathbb{Q}$ is an equation of the form

$$y^2 = x^3 + ax + b,$$

where a and b are rational parameters.

The set of solutions to an elliptic curve equation is equipped with a natural structure of an *abelian group*, and this is in large part what singles out elliptic curves for special study.

Elliptic curves

Definition

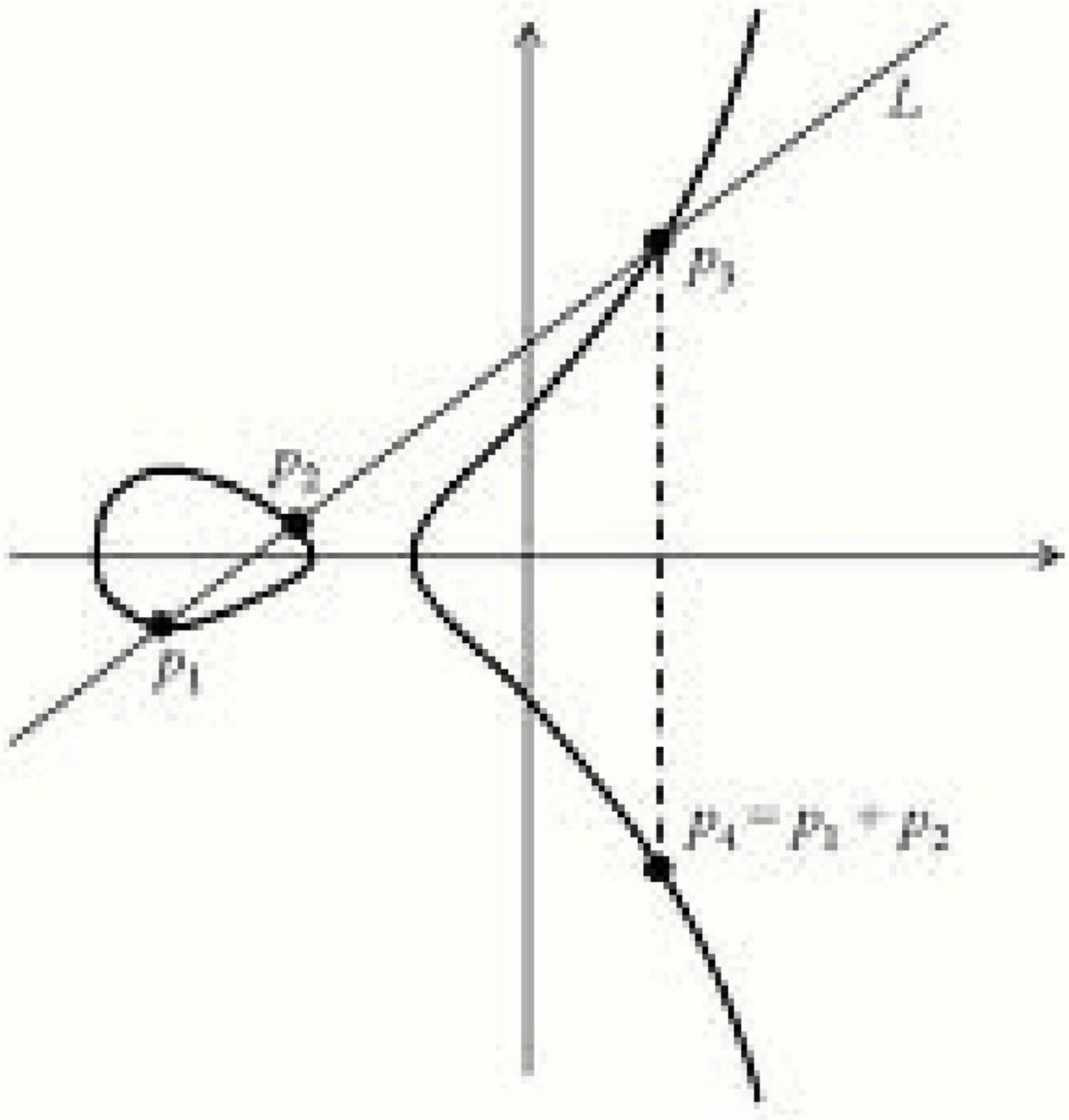
An *elliptic curve* over $\mathbb{Q}$ is an equation of the form

$$y^2 = x^3 + ax + b,$$

where a and b are rational parameters.

The set of solutions to an elliptic curve equation is equipped with a natural structure of an *abelian group*, and this is in large part what singles out elliptic curves for special study.

The addition law (over $\mathbb{R}$)



The addition law over $\mathbb{Q}$

The addition law makes it possible to generate *new rational solutions* from previously known ones: if (x_1, y_1) and (x_2, y_2) are rational solutions, then the pair (x_3, y_3) given by

$$\begin{aligned} x_3 &= \left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2 - x_1 - x_2; \\ y_3 &= y_1 + \left(\frac{y_1 - y_2}{x_1 - x_2}\right)(x_3 - x_1) \end{aligned}$$

is yet another rational solution.

Consequence: The $\mathbb{F}_p$-vector space

$$E[p] := E(\bar{\mathbb{Q}})[p] = \{Q \in E(\bar{\mathbb{Q}}) \quad pQ = 0\}$$

is equipped with a natural *linear* action of $G_{\mathbb{Q}} := \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

The addition law over $\mathbb{Q}$

The addition law makes it possible to generate *new rational solutions* from previously known ones: if (x_1, y_1) and (x_2, y_2) are rational solutions, then the pair (x_3, y_3) given by

$$\begin{aligned} x_3 &= \left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2 - x_1 - x_2; \\ y_3 &= y_1 + \left(\frac{y_1 - y_2}{x_1 - x_2}\right)(x_3 - x_1) \end{aligned}$$

is yet another rational solution.

Consequence: The $\mathbb{F}_p$-vector space

$$E[p] := E(\bar{\mathbb{Q}})[p] = \{Q \in E(\bar{\mathbb{Q}}) \quad pQ = 0\}$$

is equipped with a natural *linear* action of $G_{\mathbb{Q}} := \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

The addition law over $\mathbb{Q}$

The addition law makes it possible to generate *new rational solutions* from previously known ones: if (x_1, y_1) and (x_2, y_2) are rational solutions, then the pair (x_3, y_3) given by

$$\begin{aligned} x_3 &= \left(\frac{y_1 - y_2}{x_1 - x_2}\right)^2 - x_1 - x_2; \\ y_3 &= y_1 + \left(\frac{y_1 - y_2}{x_1 - x_2}\right)(x_3 - x_1) \end{aligned}$$

is yet another rational solution.

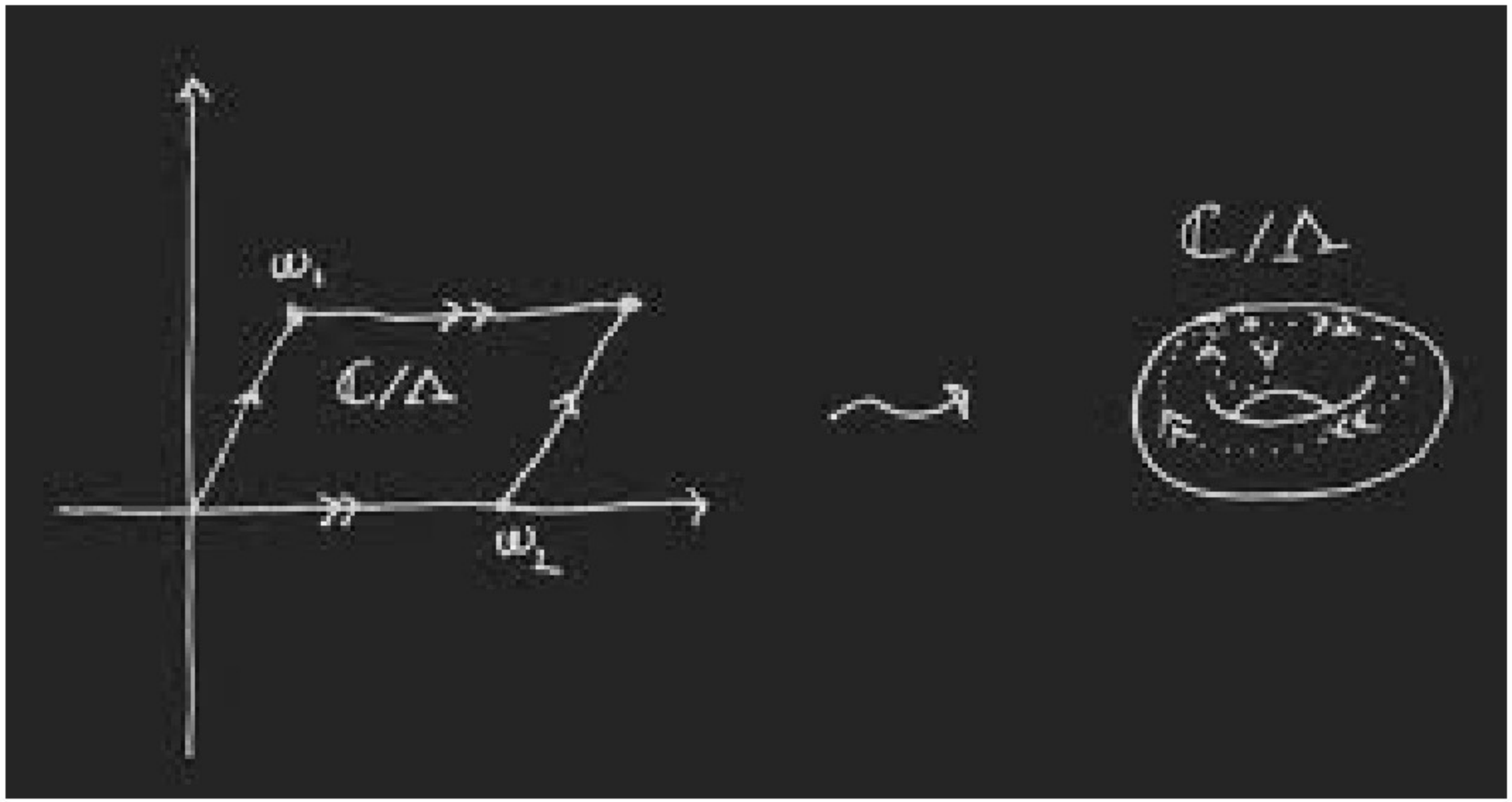
Consequence: The $\mathbb{F}_p$-vector space

$$E[p] := E(\bar{\mathbb{Q}})[p] = \{Q \in E(\bar{\mathbb{Q}}) \quad pQ = 0\}$$

is equipped with a natural *linear* action of $G_{\mathbb{Q}} := \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

The addition law over $\mathbb{C}$

Weierstrass theory identifies the abelian group $E(\mathbb{C})$ with $\mathbb{C}/\Lambda$ where Λ is a *lattice*.



Mod p Galois representations

A consequence of the complex description of the addition law is that

$$E(\mathbb{C})[p] = \frac{1}{p}\Lambda/\Lambda \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

The same is true when $\mathbb{C}$ is replaced by $\bar{\mathbb{Q}}$. Hence

$$E[p] := E(\bar{\mathbb{Q}})[p]$$

is a *two-dimensional vector space* over the field with p elements. Recall from the previous slide that it is equipped with a continuous linear action of $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

Theorem (Serre, Mazur)

The representation $E[p]$ is irreducible if p is large enough ($p > 11$).

Mod p Galois representations

A consequence of the complex description of the addition law is that

$$E(\mathbb{C})[p] = \frac{1}{p}\Lambda/\Lambda \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

The same is true when $\mathbb{C}$ is replaced by $\bar{\mathbb{Q}}$. Hence

$$E[p] := E(\bar{\mathbb{Q}})[p]$$

is a *two-dimensional vector space* over the field with p elements. Recall from the previous slide that it is equipped with a continuous linear action of $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

Theorem (Serre, Mazur)

The representation $E[p]$ is irreducible if p is large enough ($p > 11$).

Mod p Galois representations

A consequence of the complex description of the addition law is that

$$E(\mathbb{C})[p] = \frac{1}{p}\Lambda/\Lambda \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

The same is true when $\mathbb{C}$ is replaced by $\bar{\mathbb{Q}}$. Hence

$$E[p] := E(\bar{\mathbb{Q}})[p]$$

is a *two-dimensional vector space* over the field with p elements.

Recall from the previous slide that it is equipped with a continuous linear action of $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

Theorem (Serre, Mazur)

The representation $E[p]$ is irreducible if p is large enough ($p > 11$).

Mod p Galois representations

A consequence of the complex description of the addition law is that

$$E(\mathbb{C})[p] = \frac{1}{p}\Lambda/\Lambda \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

The same is true when $\mathbb{C}$ is replaced by $\bar{\mathbb{Q}}$. Hence

$$E[p] := E(\bar{\mathbb{Q}})[p]$$

is a *two-dimensional vector space* over the field with p elements. Recall from the previous slide that it is equipped with a continuous linear action of $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

Theorem (Serre, Mazur)

The representation $E[p]$ is irreducible if p is large enough ($p > 11$).

Mod p Galois representations

A consequence of the complex description of the addition law is that

$$E(\mathbb{C})[p] = \frac{1}{p}\Lambda/\Lambda \simeq \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

The same is true when $\mathbb{C}$ is replaced by $\bar{\mathbb{Q}}$. Hence

$$E[p] := E(\bar{\mathbb{Q}})[p]$$

is a *two-dimensional vector space* over the field with p elements. Recall from the previous slide that it is equipped with a continuous linear action of $G_{\mathbb{Q}} = \mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$.

Theorem (Serre, Mazur)

The representation $E[p]$ is irreducible if p is large enough ($p > 11$).

What is special about Frey's elliptic curve?

Proposition (Frey)

The representation $E_{a,b,c}[p]$ behaves as if *$E_{a,b,c}$ had non-singular reduction modulo* all primes *$\ell \neq 2$, including the odd primes dividing abc.* *(More precisely, it is* unramified *at all primes $\ell \neq 2, p$ and is (*cristalline*) at p.)*

Conjecture (Serre, 1985)

The representation $E_{a,b,c}[p]$—and hence, the curve $E_{a,b,c}$ itself!—does not exist.

What is special about Frey's elliptic curve?

Proposition (Frey)

The representation $E_{a,b,c}[p]$ *behaves* as if $E_{a,b,c}$ *had non-singular reduction modulo* all primes $\ell \neq 2$, *including the odd primes dividing abc. (More precisely, it is* unramified *at all primes* $\ell \neq 2, p$ *and is (*cristalline*) at p.)*

Conjecture (Serre, 1985)

The representation $E_{a,b,c}[p]$*—and hence, the curve* $E_{a,b,c}$ *itself!—does not exist.*

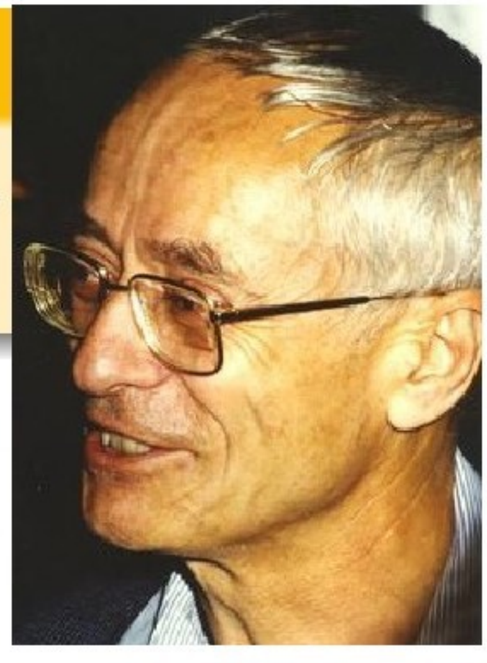
What is special about Frey's elliptic curve?

Proposition (Frey)

The representation $E_{a,b,c}[p]$ *behaves* as if $E_{a,b,c}$ *had non-singular reduction modulo* all primes $\ell \neq 2$, *including the odd primes dividing abc. (More precisely, it is* unramified *at all primes* $\ell \neq 2, p$ *and is (*cristalline*) at p.)*

Conjecture (Serre, 1985)

The representation $E_{a,b,c}[p]$*—and hence, the curve* $E_{a,b,c}$ *itself!—does not exist.*



Summary

Solutions of FLT $\Rightarrow$ Frey curves

$\Rightarrow$ Galois representations

To a solution (a, b, c) to $x^p + y^p = z^p$, we associate the *Frey elliptic curve* $E_{a,b,c}$, an equation whose arithmetic complexity depends on (a, b, c).

By passing to the mod p Galois representation $E_{a,b,c}[p]$, one obtains an object whose—*very low*—arithmetic complexity does not depend on (a, b, c) at all.

It now "suffices" to show that this Galois representation cannot exist: this is what Wiles did, by relating $E[p]$ to *modular forms*.

Summary

Solutions of FLT $\Rightarrow$ Frey curves

$\Rightarrow$ Galois representations

To a solution (a, b, c) to $x^p + y^p = z^p$, we associate the *Frey elliptic curve* $E_{a,b,c}$, an equation whose arithmetic complexity depends on (a, b, c).

By passing to the mod p Galois representation $E_{a,b,c}[p]$, one obtains an object whose—*very low*—arithmetic complexity does not depend on (a, b, c) at all.

It now "suffices" to show that this Galois representation cannot exist: this is what Wiles did, by relating $E[p]$ to *modular forms*.

Summary

$$\text{Solutions of FLT} \quad \Rightarrow \quad \text{Frey curves}$$
$$\Rightarrow \quad \text{Galois representations}$$

To a solution (a, b, c) to $x^p + y^p = z^p$, we associate the *Frey elliptic curve* $E_{a,b,c}$, an equation whose arithmetic complexity depends on (a, b, c).

By passing to the mod p Galois representation $E_{a,b,c}[p]$, one obtains an object whose—*very low*—arithmetic complexity does not depend on (a, b, c) at all.

It now "suffices" to show that this Galois representation cannot exist: this is what Wiles did, by relating $E[p]$ to *modular forms*.

Summary

$$\begin{aligned} \text{Solutions of FLT} &\Rightarrow \text{Frey curves} \\ &\Rightarrow \text{Galois representations} \end{aligned}$$

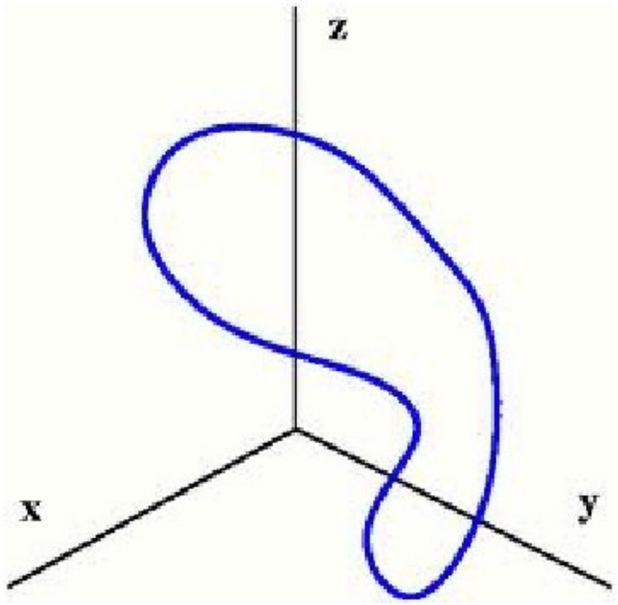
To a solution (a, b, c) to $x^p + y^p = z^p$, we associate the *Frey elliptic curve* $E_{a,b,c}$, an equation whose arithmetic complexity depends on (a, b, c).

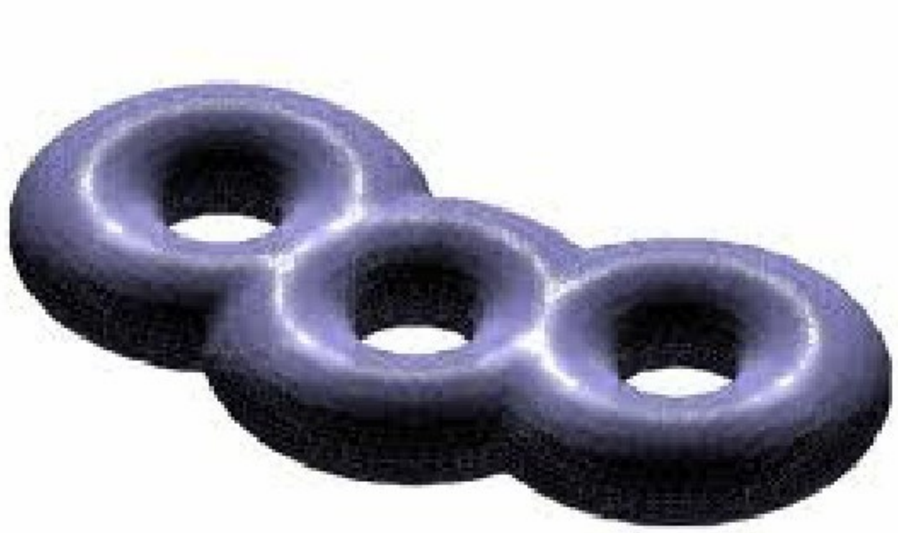
By passing to the mod p Galois representation $E_{a,b,c}[p]$, one obtains an object whose—*very low*—arithmetic complexity does not depend on (a, b, c) at all.

It now "suffices" to show that this Galois representation cannot exist: this is what Wiles did, by relating $E[p]$ to *modular forms*.

Curves

A *curve* over $\mathbb{Q}$ is a diophantine equation X whose underlying solution set over $\mathbb{R}$ is one-dimensional–and hence, whose underlying solution set over $\mathbb{C}$ is a *Riemann surface*. E.g., $f(x, y) = 0$.





Faltings' theorem, a.k.a. the Mordell conjecture

Theorem (Faltings)

Let X be a curve. Then $X(K)$ is finite for all number fields K if and only if genus$(X(\mathbb{C})) \geq 2$.

Parshin's "trick"

Parshin: To a rational solution of X—i.e., a point $a \in X(\mathbb{Q})$—one can associate an *auxiliary curve* X_a with the following properties:

1. The assignment $a \mapsto X_a$ is injective;

2. The genus $g > 1$ of X_a depends only on X and not on a;

3. The *arithmetic complexity* of X_a—i.e., the set of primes modulo which is acquires singular reduction—depends only on X as well.

Mordell's conjecture is now a consequence of

Conjecture (Shafarevich)

The set of (isomorphism classes of) curves of genus g and good reduction outside a fixed finite set of primes is finite.

Parshin's "trick"

Parshin: To a rational solution of X—i.e., a point $a \in X(\mathbb{Q})$—one can associate an *auxiliary curve* X_a with the following properties:

1. The assignment $a \mapsto X_a$ is injective;

2. The genus $g > 1$ of X_a depends only on X and not on a;

3. The *arithmetic complexity* of X_a—i.e., the set of primes modulo which is acquires singular reduction—depends only on X as well.

Mordell's conjecture is now a consequence of

Conjecture (Shafarevich)

The set of (isomorphism classes of) curves of genus g and good reduction outside a fixed finite set of primes is finite.

Parshin's "trick"

Parshin: To a rational solution of X—i.e., a point $a \in X(\mathbb{Q})$—one can associate an *auxiliary curve* X_a with the following properties:

1. The assignment $a \mapsto X_a$ is injective;

2. The genus $g > 1$ of X_a depends only on X and not on a;

3. The *arithmetic complexity* of X_a—i.e., the set of primes modulo which is acquires singular reduction—depends only on X as well.

Mordell's conjecture is now a consequence of

Conjecture (Shafarevich)

The set of (isomorphism classes of) curves of genus g and good reduction outside a fixed finite set of primes is finite.

Parshin's "trick"

Parshin: To a rational solution of X—i.e., a point $a \in X(\mathbb{Q})$—one can associate an *auxiliary curve* X_a with the following properties:

1. The assignment $a \mapsto X_a$ is injective;

2. The genus $g > 1$ of X_a depends only on X and not on a;

3. The *arithmetic complexity* of X_a—i.e., the set of primes modulo which is acquires singular reduction—depends only on X as well.

Mordell's conjecture is now a consequence of

Conjecture (Shafarevich)

The set of (isomorphism classes of) curves of genus g and good reduction outside a fixed finite set of primes is finite.

Parshin's "trick"

Parshin: To a rational solution of X—i.e., a point $a \in X(\mathbb{Q})$—one can associate an *auxiliary curve* X_a with the following properties:

1. The assignment $a \mapsto X_a$ is injective;

2. The genus $g > 1$ of X_a depends only on X and not on a;

3. The *arithmetic complexity* of X_a—i.e., the set of primes modulo which is acquires singular reduction—depends only on X as well.

Mordell's conjecture is now a consequence of

Conjecture (Shafarevich)

The set of (isomorphism classes of) curves of genus g and good reduction outside a fixed finite set of primes is finite.

Passing to the Jacobian

To bound the number of curves X_a which could arise, Faltings considers the *Jacobian*

$$J_a := \mathrm{Jac}(X_a) = \frac{\text{degree 0 divisors on } X_a}{\text{principal divisors on } X_a}.$$

It is an *abelian variety* of dimension g over $\mathbb{Q}$: a higher dimensional analogue of an elliptic curve.

Theorem (Torelli)

The assignment $X \mapsto Jac(X)$ is finite-to-one.

Passing to the Jacobian

To bound the number of curves X_a which could arise, Faltings considers the *Jacobian*

$$J_a := \mathrm{Jac}(X_a) = \frac{\text{degree 0 divisors on } X_a}{\text{principal divisors on } X_a}.$$

It is an *abelian variety* of dimension g over $\mathbb{Q}$: a higher dimensional analogue of an elliptic curve.

Theorem (Torelli)

The assignment $X \mapsto Jac(X)$ is finite-to-one.

Passing to the Jacobian

To bound the number of curves X_a which could arise, Faltings considers the *Jacobian*

$$J_a := \mathrm{Jac}(X_a) = \frac{\text{degree 0 divisors on } X_a}{\text{principal divisors on } X_a}.$$

It is an *abelian variety* of dimension g over $\mathbb{Q}$: a higher dimensional analogue of an elliptic curve.

Theorem (Torelli)

The assignment $X \mapsto Jac(X)$ is finite-to-one.

Galois representations

As in Wiles' proof of FLT, Galois representations play a key role.

$$\cdots \to J_a[p^n] \to J_a[p^{n-1}] \to \cdots \to J_a[p^2] \to J_a[p].$$

As abelian groups,

$$J_a[p^\infty] := \varprojlim J_a[p^n] \simeq \mathbb{Z}_p^{2g}.$$

$$V_{a,p} := J_a[p^\infty] \otimes \mathbb{Q}_p \simeq \mathbb{Q}_p^{2g}.$$

These groups and vector spaces are equipped with a continuous linear action of $G_{\mathbb{Q}}$.

Galois representations

As in Wiles' proof of FLT, Galois representations play a key role.

$$\cdots \to J_a[p^n] \to J_a[p^{n-1}] \to \cdots \to J_a[p^2] \to J_a[p].$$

As abelian groups,

$$J_a[p^\infty] := \varprojlim J_a[p^n] \simeq \mathbb{Z}_p^{2g}.$$

$$V_{a,p} := J_a[p^\infty] \otimes \mathbb{Q}_p \simeq \mathbb{Q}_p^{2g}.$$

These groups and vector spaces are equipped with a continuous linear action of $G_{\mathbb{Q}}$.

Galois representations

As in Wiles' proof of FLT, Galois representations play a key role.

$$\cdots \to J_a[p^n] \to J_a[p^{n-1}] \to \cdots \to J_a[p^2] \to J_a[p].$$

As abelian groups,

$$J_a[p^\infty] := \varprojlim J_a[p^n] \simeq \mathbb{Z}_p^{2g}.$$

$$V_{a,p} := J_a[p^\infty] \otimes \mathbb{Q}_p \simeq \mathbb{Q}_p^{2g}.$$

These groups and vector spaces are equipped with a continuous linear action of $G_{\mathbb{Q}}$.

Galois representations

As in Wiles' proof of FLT, Galois representations play a key role.

$$\cdots \to J_a[p^n] \to J_a[p^{n-1}] \to \cdots \to J_a[p^2] \to J_a[p].$$

As abelian groups,

$$J_a[p^\infty] := \varprojlim J_a[p^n] \simeq \mathbb{Z}_p^{2g}.$$

$$V_{a,p} := J_a[p^\infty] \otimes \mathbb{Q}_p \simeq \mathbb{Q}_p^{2g}.$$

These groups and vector spaces are equipped with a continuous linear action of $G_{\mathbb{Q}}$.

Galois representations

As in Wiles' proof of FLT, Galois representations play a key role.

$$\cdots \to J_a[p^n] \to J_a[p^{n-1}] \to \cdots \to J_a[p^2] \to J_a[p].$$

As abelian groups,

$$J_a[p^\infty] := \varprojlim J_a[p^n] \simeq \mathbb{Z}_p^{2g}.$$

$$V_{a,p} := J_a[p^\infty] \otimes \mathbb{Q}_p \simeq \mathbb{Q}_p^{2g}.$$

These groups and vector spaces are equipped with a continuous linear action of $G_{\mathbb{Q}}$.

Cohomological interpretation

The representations $J_a[p^\infty]$ and $V_{a,p}$ admit a cohomological interpretation.

If $g = 1$, so that $X(\mathbb{C}) = \mathbb{C}/\Lambda$, then

$$J_a[p^\infty] = \varinjlim \frac{1}{p^n}\Lambda/\Lambda = \varprojlim \Lambda/p^n\Lambda = \Lambda \otimes \mathbb{Z}_p = H_1(E(\mathbb{C}), \mathbb{Z}_p).$$

For arbitrary g,

$$H_1(X, \mathbb{Q}_p) := \mathrm{Jac}(X)[p^\infty] \otimes \mathbb{Q}_p$$

is equipped with a continuous linear action of $G_{\mathbb{Q}}$.

Hence $H_1(-, \mathbb{Q}_p)$ is a functor from the category of curves over $\mathbb{Q}$ to the category of continuous linear representations of $G_{\mathbb{Q}}$.

Cohomological interpretation

The representations $J_a[p^\infty]$ and $V_{a,p}$ admit a cohomological interpretation.

If $g = 1$, so that $X(\mathbb{C}) = \mathbb{C}/\Lambda$, then

$$J_a[p^\infty] = \varprojlim \frac{1}{p^n}\Lambda/\Lambda = \varprojlim \Lambda/p^n\Lambda = \Lambda \otimes \mathbb{Z}_p = H_1(E(\mathbb{C}), \mathbb{Z}_p).$$

For arbitrary g,

$$H_1(X, \mathbb{Q}_p) := \mathrm{Jac}(X)[p^\infty] \otimes \mathbb{Q}_p$$

is equipped with a continuous linear action of $G_{\mathbb{Q}}$.

Hence $H_1(-, \mathbb{Q}_p)$ is a functor from the category of curves over $\mathbb{Q}$ to the category of continuous linear representations of $G_{\mathbb{Q}}$.

Cohomological interpretation

The representations $J_a[p^\infty]$ and $V_{a,p}$ admit a cohomological interpretation.

If $g = 1$, so that $X(\mathbb{C}) = \mathbb{C}/\Lambda$, then

$$J_a[p^\infty] = \varprojlim \frac{1}{p^n}\Lambda/\Lambda = \varprojlim \Lambda/p^n\Lambda = \Lambda \otimes \mathbb{Z}_p = H_1(E(\mathbb{C}), \mathbb{Z}_p).$$

For arbitrary g,

$$H_1(X, \mathbb{Q}_p) := \mathrm{Jac}(X)[p^\infty] \otimes \mathbb{Q}_p$$

is equipped with a continuous linear action of $G_{\mathbb{Q}}$.

Hence $H_1(-, \mathbb{Q}_p)$ is a functor from the category of curves over $\mathbb{Q}$ to the category of continuous linear representations of $G_{\mathbb{Q}}$.

Cohomological interpretation

The representations $J_a[p^\infty]$ and $V_{a,p}$ admit a cohomological interpretation.

If $g = 1$, so that $X(\mathbb{C}) = \mathbb{C}/\Lambda$, then

$$J_a[p^\infty] = \varprojlim \frac{1}{p^n}\Lambda/\Lambda = \varprojlim \Lambda/p^n\Lambda = \Lambda \otimes \mathbb{Z}_p = H_1(E(\mathbb{C}), \mathbb{Z}_p).$$

For arbitrary g,

$$H_1(X, \mathbb{Q}_p) := \mathrm{Jac}(X)[p^\infty] \otimes \mathbb{Q}_p$$

is equipped with a continuous linear action of $G_{\mathbb{Q}}$.

Hence $H_1(-, \mathbb{Q}_p)$ is a functor from the category of curves over $\mathbb{Q}$ to the category of continuous linear representations of $G_{\mathbb{Q}}$.

Etale cohomology

The extra structure on $H_1(X, \mathbb{Q}_p)$ given by the $G_{\mathbb{Q}}$-action carries a great deal of information about X.

1. For all $\ell \neq p$ at which X has good reduction, the representation $H_1(X, \mathbb{Q}_p)$ is unramified at ℓ, and the characteristic polynomial $P_\ell(x) \in \mathbb{Q}_p[x]$ of the frobenius element σ_ℓ at ℓ belongs to $\mathbb{Z}[x]$ and is independent of p.
2. Lefshetz fixed point formula

$$\#X(\mathbb{F}_\ell) = \ell + 1 - \mathrm{trace}(\sigma_\ell|_{H_1(X,\mathbb{Q}_p)}).$$

Etale cohomology

The extra structure on $H_1(X, \mathbb{Q}_p)$ given by the $G_{\mathbb{Q}}$-action carries a great deal of information about X.

1. For all $\ell \neq p$ at which X has good reduction, the representation $H_1(X, \mathbb{Q}_p)$ is unramified at ℓ, and the characteristic polynomial $P_\ell(x) \in \mathbb{Q}_p[x]$ of the frobenius element σ_ℓ at ℓ belongs to $\mathbb{Z}[x]$ and is independent of p.
2. Lefshetz fixed point formula

$$\#X(\mathbb{F}_\ell) = \ell + 1 - \mathrm{trace}(\sigma_\ell|_{H_1(X,\mathbb{Q}_p)}).$$

Etale cohomology

The extra structure on $H_1(X, \mathbb{Q}_p)$ given by the $G_{\mathbb{Q}}$-action carries a great deal of information about X.

1. For all $\ell \neq p$ at which X has good reduction, the representation $H_1(X, \mathbb{Q}_p)$ is unramified at ℓ, and the characteristic polynomial $P_\ell(x) \in \mathbb{Q}_p[x]$ of the frobenius element σ_ℓ at ℓ belongs to $\mathbb{Z}[x]$ and is independent of p.
2. Lefshetz fixed point formula

$$\#X(\mathbb{F}_\ell) = \ell + 1 - \mathrm{trace}(\sigma_\ell|_{H_1(X,\mathbb{Q}_p)}).$$

Etale cohomology

The extra structure on $H_1(X, \mathbb{Q}_p)$ given by the $G_{\mathbb{Q}}$-action carries a great deal of information about X.

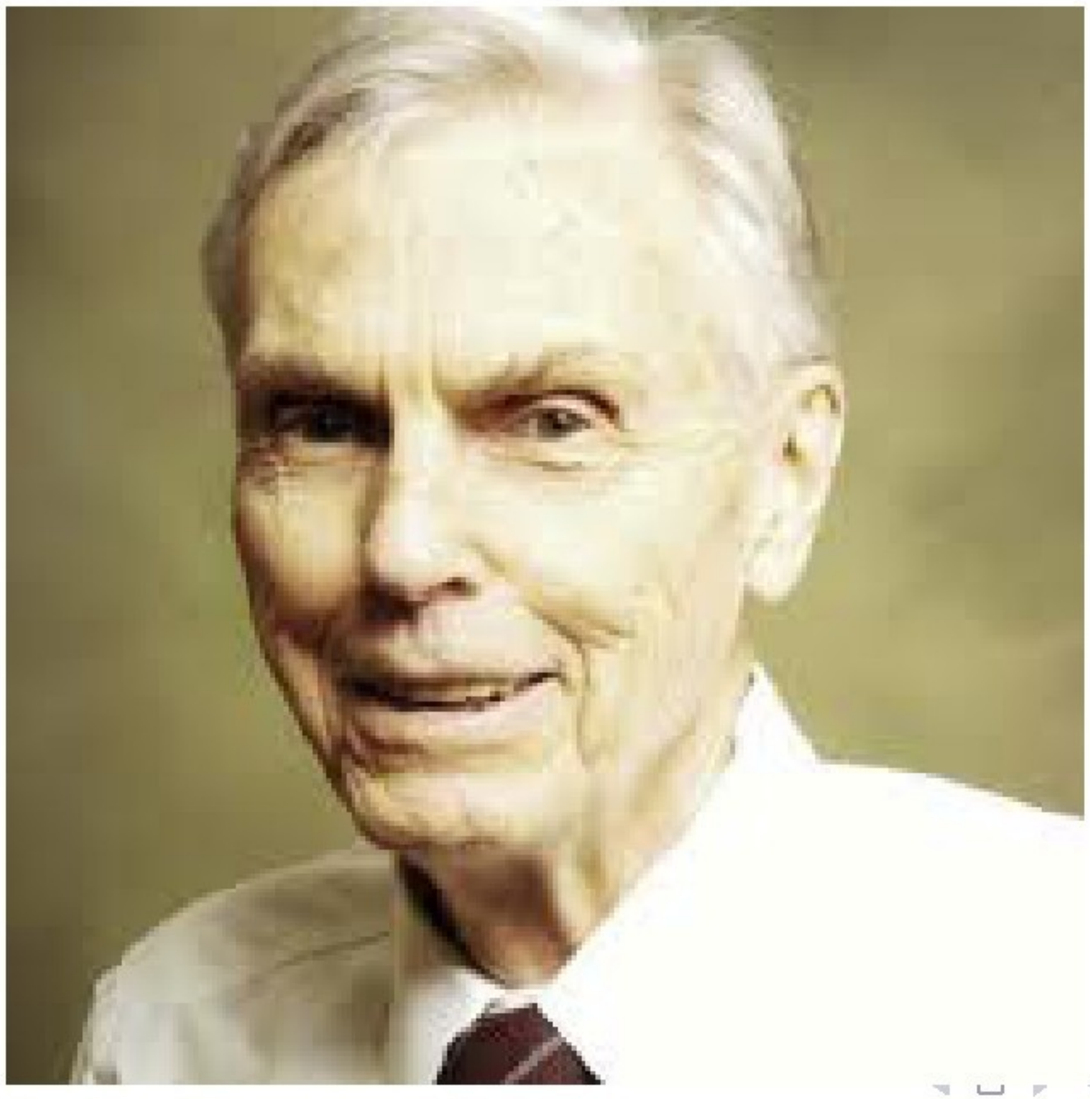
1. For all $\ell \neq p$ at which X has good reduction, the representation $H_1(X, \mathbb{Q}_p)$ is unramified at ℓ, and the characteristic polynomial $P_\ell(x) \in \mathbb{Q}_p[x]$ of the frobenius element σ_ℓ at ℓ belongs to $\mathbb{Z}[x]$ and is independent of p.
2. Lefshetz fixed point formula

$$\#X(\mathbb{F}_\ell) = \ell + 1 - \mathrm{trace}(\sigma_\ell|_{H_1(X,\mathbb{Q}_p)}).$$

The Tate conjecture

Conjecture (Tate)

If $H_1(X_1, \mathbb{Q}_p) \simeq H_1(X_2, \mathbb{Q}_p)$, *then there is a finite morphism* $Jac(X_1) \longrightarrow Jac(X_2)$.



Faltings' finiteness theorems

Theorem (Faltings)

1. *The Tate conjecture is true, and there are finitely many abelian varieties varieties in a given isogeny class. In particular, the assignment $a \mapsto H_1(X_a, \mathbb{Q}_p)$ is finite-to-one.*
2. *The representation $H_1(X, \mathbb{Q}_p)$ is semi-simple, and there are finitely many rational semi-simple p-adic representations of $G_{\mathbb{Q}}$ with "bounded arithmetic complexity", up to isomorphism.*

Faltings' finiteness theorems

Theorem (Faltings)

1. *The Tate conjecture is true, and there are finitely many abelian varieties varieties in a given isogeny class. In particular, the assignment* $a \mapsto H_1(X_a, \mathbb{Q}_p)$ *is finite-to-one.*
2. *The representation* $H_1(X, \mathbb{Q}_p)$ *is semi-simple, and there are finitely many rational semi-simple p-adic representations of* $G_{\mathbb{Q}}$ *with "bounded arithmetic complexity", up to isomorphism.*

Faltings' finiteness theorems

Theorem (Faltings)

1. *The Tate conjecture is true, and there are finitely many abelian varieties varieties in a given isogeny class. In particular, the assignment $a \mapsto H_1(X_a, \mathbb{Q}_p)$ is finite-to-one.*
2. *The representation $H_1(X, \mathbb{Q}_p)$ is semi-simple, and there are finitely many rational semi-simple p-adic representations of $G_{\mathbb{Q}}$ with "bounded arithmetic complexity", up to isomorphism.*

Faltings' finiteness theorems

Theorem (Faltings)

1. *The Tate conjecture is true, and there are finitely many abelian varieties varieties in a given isogeny class. In particular, the assignment* $a \mapsto H_1(X_a, \mathbb{Q}_p)$ *is finite-to-one.*
2. *The representation* $H_1(X, \mathbb{Q}_p)$ *is semi-simple, and there are finitely many rational semi-simple p-adic representations of* $G_{\mathbb{Q}}$ *with "bounded arithmetic complexity", up to isomorphism.*

Faltings' finiteness theorems

Theorem (Faltings)

1. *The Tate conjecture is true, and there are finitely many abelian varieties varieties in a given isogeny class. In particular, the assignment* $a \mapsto H_1(X_a, \mathbb{Q}_p)$ *is finite-to-one.*
2. *The representation* $H_1(X, \mathbb{Q}_p)$ *is semi-simple, and there are finitely many rational semi-simple p-adic representations of* $G_{\mathbb{Q}}$ *with "bounded arithmetic complexity", up to isomorphism.*

Faltings' finiteness theorems

Theorem (Faltings)

1. *The Tate conjecture is true, and there are finitely many abelian varieties varieties in a given isogeny class. In particular, the assignment* $a \mapsto H_1(X_a, \mathbb{Q}_p)$ *is finite-to-one.*
2. *The representation* $H_1(X, \mathbb{Q}_p)$ *is semi-simple, and there are finitely many rational semi-simple p-adic representations of* $G_{\mathbb{Q}}$ *with "bounded arithmetic complexity", up to isomorphism.*

Summary of Faltings' proof

Rational points $a \in X(\mathbb{Q})$ $\Rightarrow$ Curves X_a

$\Rightarrow$ Abelian varieties J_a

$\Rightarrow$ Galois representations $H_1(X_a, \mathbb{Q}_p)$

The various finiteness theorems of Faltings are combined to show that each of the above assignments is finite-to-one, and that the target of the last assignment is finite.

Summary of Faltings' proof

Rational points $a \in X(\mathbb{Q})$ $\Rightarrow$ Curves X_a

$\Rightarrow$ Abelian varieties J_a

$\Rightarrow$ Galois representations $H_1(X_a, \mathbb{Q}_p)$

The various finiteness theorems of Faltings are combined to show that each of the above assignments is finite-to-one, and that the target of the last assignment is finite.

Summary of Faltings' proof

Rational points $a \in X(\mathbb{Q})$ $\Rightarrow$ Curves X_a

$\Rightarrow$ Abelian varieties J_a

$\Rightarrow$ Galois representations $H_1(X_a, \mathbb{Q}_p)$

The various finiteness theorems of Faltings are combined to show that each of the above assignments is finite-to-one, and that the target of the last assignment is finite.

Summary of Faltings' proof

Rational points $a \in X(\mathbb{Q})$ $\Rightarrow$ Curves X_a

$\Rightarrow$ Abelian varieties J_a

$\Rightarrow$ Galois representations $H_1(X_a, \mathbb{Q}_p)$

The various finiteness theorems of Faltings are combined to show that each of the above assignments is finite-to-one, and that the target of the last assignment is finite.

Summary of Faltings' proof

$$\begin{aligned}
\text{Rational points } a \in X(\mathbb{Q}) \quad &\Rightarrow \quad \text{Curves } X_a \\
&\Rightarrow \quad \text{Abelian varieties } J_a \\
&\Rightarrow \quad \text{Galois representations } H_1(X_a, \mathbb{Q}_p)
\end{aligned}$$

The various finiteness theorems of Faltings are combined to show that each of the above assignments is finite-to-one, and that the target of the last assignment is finite.

Constructing points

The results described above illustrate settings where one tries to bound the set of solutions to Diophantine equations *from above*,

1. by showing there are no solutions at all, as in Wiles' proof of Fermat's Last Theorem;
2. by showing there are finitely many solutions, as in Faltings' proof of the Mordell conjecture.

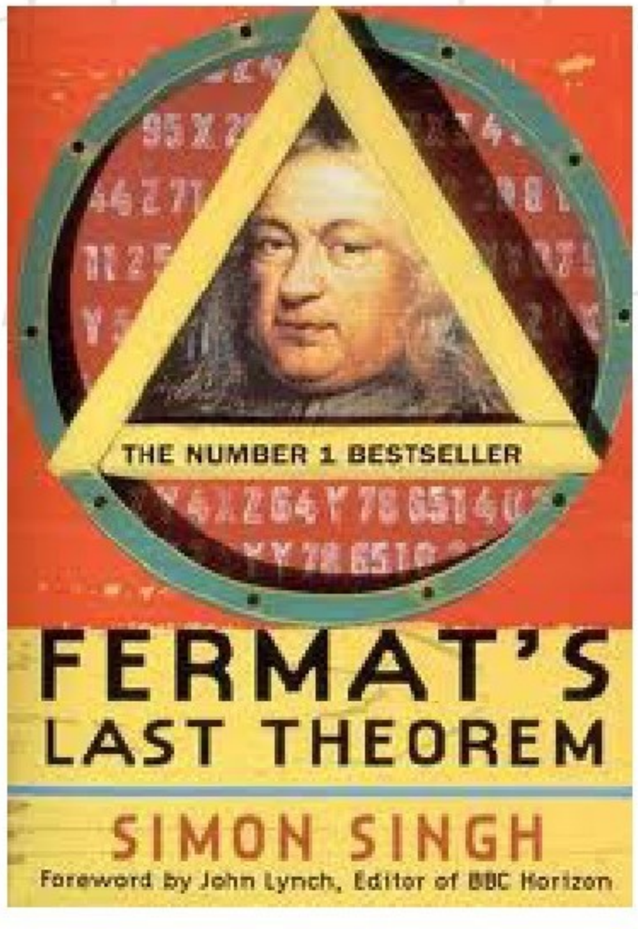
What about the *construction* of explicit solutions?

Constructing points

The results described above illustrate settings where one tries to bound the set of solutions to Diophantine equations *from above*,

1. by showing there are no solutions at all, as in Wiles' proof of Fermat's Last Theorem;
2. by showing there are finitely many solutions, as in Faltings' [illegible] Mordell co[illegible]

[illegible] construction[illegible]ns?



Constructing points

The results described above illustrate settings where one tries to bound the set of solutions to Diophantine equations *from above*,

1. by showing there are no solutions at all, as in Wiles' proof of Fermat's Last Theorem;
2. by showing there are finitely many solutions, as in Faltings' proof of the Mordell conjecture.

Constructing points

The results described above illustrate settings where one tries to bound the set of solutions to Diophantine equations *from above*,

1. by showing there are no solutions at all, as in Wiles' proof of Fermat's Last Theorem;
2. by showing there are finitely many solutions, as in Faltings' proof of the Mordell conjecture.

What about the *construction* of explicit solutions?

Elliptic curves

We consider only the simplest non-trivial setting: an elliptic curve E over $\mathbb{Q}$ (with good reduction outside a finite set S of primes).

Given $a \in E(\mathbb{Q})$, the most natural variety one can associate to it is the *open curve*

$$E_a := E - \{0, a\}.$$

Its homology and cohomology with coefficients in L fit into functorial ("excision") exact sequences

$$0 \longrightarrow L(1) \longrightarrow H_1(E_a) \longrightarrow H_1(E) \longrightarrow 0,$$

$$0 \longrightarrow H^1(E) \longrightarrow H^1(E_a) \longrightarrow L(-1) \longrightarrow 0.$$

Elliptic curves

We consider only the simplest non-trivial setting: an elliptic curve E over $\mathbb{Q}$ (with good reduction outside a finite set S of primes). Given $a \in E(\mathbb{Q})$, the most natural variety one can associate to it is the *open curve*

$$E_a := E - \{0, a\}.$$

Its homology and cohomology with coefficients in L fit into functorial ("excision") exact sequences

$$0 \longrightarrow L(1) \longrightarrow H_1(E_a) \longrightarrow H_1(E) \longrightarrow 0,$$

$$0 \longrightarrow H^1(E) \longrightarrow H^1(E_a) \longrightarrow L(-1) \longrightarrow 0.$$

Elliptic curves

We consider only the simplest non-trivial setting: an elliptic curve E over $\mathbb{Q}$ (with good reduction outside a finite set S of primes). Given $a \in E(\mathbb{Q})$, the most natural variety one can associate to it is the *open curve*

$$E_a := E - \{0, a\}.$$

Its homology and cohomology with coefficients in L fit into functorial ("excision") exact sequences

$$0 \longrightarrow L(1) \longrightarrow H_1(E_a) \longrightarrow H_1(E) \longrightarrow 0,$$

$$0 \longrightarrow H^1(E) \longrightarrow H^1(E_a) \longrightarrow L(-1) \longrightarrow 0.$$

Elliptic curves

We consider only the simplest non-trivial setting: an elliptic curve E over $\mathbb{Q}$ (with good reduction outside a finite set S of primes). Given $a \in E(\mathbb{Q})$, the most natural variety one can associate to it is the *open curve*

$$E_a := E - \{0, a\}.$$

Its homology and cohomology with coefficients in L fit into functorial ("excision") exact sequences

$$0 \longrightarrow L(1) \longrightarrow H_1(E_a) \longrightarrow H_1(E) \longrightarrow 0,$$

$$0 \longrightarrow H^1(E) \longrightarrow H^1(E_a) \longrightarrow L(-1) \longrightarrow 0.$$

Elliptic curves

We consider only the simplest non-trivial setting: an elliptic curve E over $\mathbb{Q}$ (with good reduction outside a finite set S of primes). Given $a \in E(\mathbb{Q})$, the most natural variety one can associate to it is the *open curve*

$$E_a := E - \{0, a\}.$$

Its homology and cohomology with coefficients in L fit into functorial ("excision") exact sequences

$$0 \longrightarrow L(1) \longrightarrow H_1(E_a) \longrightarrow H_1(E) \longrightarrow 0,$$

$$0 \longrightarrow H^1(E) \longrightarrow H^1(E_a) \longrightarrow L(-1) \longrightarrow 0.$$

The many faces of cohomology theories

In (arithmetic) algebraic geometry, cohomology functors come in many guises, and are equipped with a plethora of extra structures:

1. The *Betti cohomology* $H^1_B(X(\mathbb{C}), \mathbb{Z}) \simeq \mathbb{Z}^{2g+s-1}$;
2. The *de Rham cohomology* $H^1_{\mathrm{dR}}(X/\mathbb{C})$ equipped with the *Hodge filtration*

$$0 \longrightarrow \Omega^1(X(\mathbb{C})) \longrightarrow H^1_{\mathrm{dR}}(X/\mathbb{C}) \longrightarrow H^1(X, \mathcal{O}_X) \longrightarrow 0$$

and the *comparison isomorphism*

$$H^1_{\mathrm{dR}}(X/\mathbb{C}) = H^1_B(X(\mathbb{C}), \mathbb{Z}) \otimes \mathbb{C}$$

sending the class of ω to the functional $\gamma \mapsto \int_\gamma \omega$.

3. The *étale cohomology* $H^1_{\mathrm{et}}(X_{\bar{\mathbb{Q}}}, \mathbb{Q}_p)$ equipped with its continuous $\mathbb{Q}_p$-linear action of the Galois group $G_{\mathbb{Q}}$.

The many faces of cohomology theories

In (arithmetic) algebraic geometry, cohomology functors come in many guises, and are equipped with a plethora of extra structures:

1. The *Betti cohomology* $H^1_B(X(\mathbb{C}), \mathbb{Z}) \simeq \mathbb{Z}^{2g+s-1}$;
2. The *de Rham cohomology* $H^1_{\mathrm{dR}}(X/\mathbb{C})$ equipped with the *Hodge filtration*

$$0 \longrightarrow \Omega^1(X(\mathbb{C})) \longrightarrow H^1_{\mathrm{dR}}(X/\mathbb{C}) \longrightarrow H^1(X, \mathcal{O}_X) \longrightarrow 0$$

and the *comparison isomorphism*

$$H^1_{\mathrm{dR}}(X/\mathbb{C}) = H^1_B(X(\mathbb{C}), \mathbb{Z}) \otimes \mathbb{C}$$

sending the class of ω to the functional $\gamma \mapsto \int_\gamma \omega$.

3. The *étale cohomology* $H^1_{\mathrm{et}}(X_{\bar{\mathbb{Q}}}, \mathbb{Q}_p)$ equipped with its continuous $\mathbb{Q}_p$-linear action of the Galois group $G_{\mathbb{Q}}$.

The many faces of cohomology theories

In (arithmetic) algebraic geometry, cohomology functors come in many guises, and are equipped with a plethora of extra structures:

1. The *Betti cohomology* $H^1_B(X(\mathbb{C}), \mathbb{Z}) \simeq \mathbb{Z}^{2g+s-1}$;
2. The *de Rham cohomology* $H^1_{\mathrm{dR}}(X/\mathbb{C})$ equipped with the *Hodge filtration*

$$0 \longrightarrow \Omega^1(X(\mathbb{C})) \longrightarrow H^1_{\mathrm{dR}}(X/\mathbb{C}) \longrightarrow H^1(X, \mathcal{O}_X) \longrightarrow 0$$

and the *comparison isomorphism*

$$H^1_{\mathrm{dR}}(X/\mathbb{C}) = H^1_B(X(\mathbb{C}), \mathbb{Z}) \otimes \mathbb{C}$$

sending the class of ω to the functional $\gamma \mapsto \int_\gamma \omega$.

3. The *étale cohomology* $H^1_{\mathrm{et}}(X_{\bar{\mathbb{Q}}}, \mathbb{Q}_p)$ equipped with its continuous $\mathbb{Q}_p$-linear action of the Galois group $G_{\mathbb{Q}}$.

The many faces of cohomology theories

In (arithmetic) algebraic geometry, cohomology functors come in many guises, and are equipped with a plethora of extra structures:

1. The *Betti cohomology* $H^1_B(X(\mathbb{C}), \mathbb{Z}) \simeq \mathbb{Z}^{2g+s-1}$;
2. The *de Rham cohomology* $H^1_{\mathrm{dR}}(X/\mathbb{C})$ equipped with the *Hodge filtration*

$$0 \longrightarrow \Omega^1(X(\mathbb{C})) \longrightarrow H^1_{\mathrm{dR}}(X/\mathbb{C}) \longrightarrow H^1(X, \mathcal{O}_X) \longrightarrow 0$$

and the *comparison isomorphism*

$$H^1_{\mathrm{dR}}(X/\mathbb{C}) = H^1_B(X(\mathbb{C}), \mathbb{Z}) \otimes \mathbb{C}$$

sending the class of ω to the functional $\gamma \mapsto \int_\gamma \omega$.

3. The *étale cohomology* $H^1_{\mathrm{et}}(X_{\bar{\mathbb{Q}}}, \mathbb{Q}_p)$ equipped with its continuous $\mathbb{Q}_p$-linear action of the Galois group $G_{\mathbb{Q}}$.

The many faces of cohomology theories

In (arithmetic) algebraic geometry, cohomology functors come in many guises, and are equipped with a plethora of extra structures:

1. The *Betti cohomology* $H^1_B(X(\mathbb{C}), \mathbb{Z}) \simeq \mathbb{Z}^{2g+s-1}$;
2. The *de Rham cohomology* $H^1_{\mathrm{dR}}(X/\mathbb{C})$ equipped with the *Hodge filtration*

$$0 \longrightarrow \Omega^1(X(\mathbb{C})) \longrightarrow H^1_{\mathrm{dR}}(X/\mathbb{C}) \longrightarrow H^1(X, \mathcal{O}_X) \longrightarrow 0$$

and the *comparison isomorphism*

$$H^1_{\mathrm{dR}}(X/\mathbb{C}) = H^1_B(X(\mathbb{C}), \mathbb{Z}) \otimes \mathbb{C}$$

sending the class of ω to the functional $\gamma \mapsto \int_\gamma \omega$.

3. The *étale cohomology* $H^1_{\mathrm{et}}(X_{\bar{\mathbb{Q}}}, \mathbb{Q}_p)$ equipped with its continuous $\mathbb{Q}_p$-linear action of the Galois group $G_{\mathbb{Q}}$.

The many faces of cohomology theories

In (arithmetic) algebraic geometry, cohomology functors come in many guises, and are equipped with a plethora of extra structures:

1. The *Betti cohomology* $H^1_B(X(\mathbb{C}), \mathbb{Z}) \simeq \mathbb{Z}^{2g+s-1}$;
2. The *de Rham cohomology* $H^1_{\mathrm{dR}}(X/\mathbb{C})$ equipped with the *Hodge filtration*

$$0 \longrightarrow \Omega^1(X(\mathbb{C})) \longrightarrow H^1_{\mathrm{dR}}(X/\mathbb{C}) \longrightarrow H^1(X, \mathcal{O}_X) \longrightarrow 0$$

and the *comparison isomorphism*

$$H^1_{\mathrm{dR}}(X/\mathbb{C}) = H^1_B(X(\mathbb{C}), \mathbb{Z}) \otimes \mathbb{C}$$

sending the class of ω to the functional $\gamma \mapsto \int_\gamma \omega$.

3. The *étale cohomology* $H^1_{\mathrm{et}}(X_{\bar{\mathbb{Q}}}, \mathbb{Q}_p)$ equipped with its continuous $\mathbb{Q}_p$-linear action of the Galois group $G_{\mathbb{Q}}$.

The many faces of cohomology theories

In (arithmetic) algebraic geometry, cohomology functors come in many guises, and are equipped with a plethora of extra structures:

1. The *Betti cohomology* $H^1_B(X(\mathbb{C}), \mathbb{Z}) \simeq \mathbb{Z}^{2g+s-1}$;
2. The *de Rham cohomology* $H^1_{\mathrm{dR}}(X/\mathbb{C})$ equipped with the *Hodge filtration*

$$0 \longrightarrow \Omega^1(X(\mathbb{C})) \longrightarrow H^1_{\mathrm{dR}}(X/\mathbb{C}) \longrightarrow H^1(X, \mathcal{O}_X) \longrightarrow 0$$

and the *comparison isomorphism*

$$H^1_{\mathrm{dR}}(X/\mathbb{C}) = H^1_B(X(\mathbb{C}), \mathbb{Z}) \otimes \mathbb{C}$$

sending the class of ω to the functional $\gamma \mapsto \int_\gamma \omega$.

3. The *étale cohomology* $H^1_{\mathrm{et}}(X_{\bar{\mathbb{Q}}}, \mathbb{Q}_p)$ equipped with its continuous $\mathbb{Q}_p$-linear action of the Galois group $G_{\mathbb{Q}}$.

Mixed Hodge structures

When X is an (open) curve, the data

$$H^1_{\mathrm{dR}}(X/\mathbb{C}) := (H^1_B(X(\mathbb{C}),\mathbb{Z}) \subset H^1_{\mathrm{dR}}(X/\mathbb{C}) \supset \Omega^1(X/\mathbb{C}))$$

is a prototypical example of an *integral (mixed) Hodge structure*.

Proposition

If E is an elliptic curve, and $a \in E(\mathbb{C})$, the mixed Hodge structure $H^1_{\mathrm{dR}}(E_a)$—more precisely, its class in $\mathrm{Ext}^1_{MHS}(\mathbb{C}(-1), H^1_{\mathrm{dR}}(E))$—determines the complex point a completely.

Indeed, the class of E_a is encoded in the complex line integral

$$\mathrm{class}(E_a) \quad \leftrightarrow \quad \int_0^a \omega_E \quad \in \quad \mathbb{C}/\Lambda_E.$$

Mixed Hodge structures

When X is an (open) curve, the data

$$H^1_{\mathrm{dR}}(X/\mathbb{C}) := (H^1_B(X(\mathbb{C}),\mathbb{Z}) \subset H^1_{\mathrm{dR}}(X/\mathbb{C}) \supset \Omega^1(X/\mathbb{C}))$$

is a prototypical example of an *integral (mixed) Hodge structure*.

Proposition

If E is an elliptic curve, and $a \in E(\mathbb{C})$, the mixed Hodge structure $H^1_{\mathrm{dR}}(E_a)$—more precisely, its class in $\mathrm{Ext}^1_{MHS}(\mathbb{C}(-1), H^1_{\mathrm{dR}}(E))$—determines the complex point a completely.

Indeed, the class of E_a is encoded in the complex line integral

$$\mathrm{class}(E_a) \quad \leftrightarrow \quad \int_0^a \omega_E \quad \in \quad \mathbb{C}/\Lambda_E.$$

Mixed Hodge structures

When X is an (open) curve, the data

$$H^1_{\mathrm{dR}}(X/\mathbb{C}) := (H^1_B(X(\mathbb{C}),\mathbb{Z}) \subset H^1_{\mathrm{dR}}(X/\mathbb{C}) \supset \Omega^1(X/\mathbb{C}))$$

is a prototypical example of an *integral (mixed) Hodge structure*.

Proposition

If E is an elliptic curve, and $a \in E(\mathbb{C})$, the mixed Hodge structure $H^1_{\mathrm{dR}}(E_a)$—more precisely, its class in $\mathrm{Ext}^1_{MHS}(\mathbb{C}(-1), H^1_{\mathrm{dR}}(E))$—determines the complex point a completely.

Indeed, the class of E_a is encoded in the complex line integral

$$\mathrm{class}(E_a) \quad \leftrightarrow \quad \int_0^a \omega_E \quad \in \quad \mathbb{C}/\Lambda_E.$$

Extensions of p-adic Galois representations

Given $a \in E(\mathbb{Q})$, the mixed Hodge structure $H^1_{\mathrm{dR}}(E_a)$ has a counterpart in the realm of p-adic Galois representations: the *étale cohomology group* $H^1_{\mathrm{et}}(E_a, \mathbb{Q}_p)$ which fits into an exact sequence

$$0 \longrightarrow H^1_{\mathrm{et}}(E, \mathbb{Q}_p) \longrightarrow H^1_{\mathrm{et}}(E_a, \mathbb{Q}_p) \longrightarrow \mathbb{Q}_p(-1) \longrightarrow 0.$$

Conjecture (Shafarevich, Tate)

If E is an elliptic curve, and ξ is a class in $\mathrm{Ext}^1_{Rep_{G_{\mathbb{Q}}}}(\mathbb{Q}_p(-1), H^1_{\mathrm{et}}(E, \mathbb{Q}_p))$ satisfying suitable explicit "local conditions", then ξ is proportional to the class of E_a, for some $a \in E(\mathbb{Q})$.

Extensions of p-adic Galois representations

Given $a \in E(\mathbb{Q})$, the mixed Hodge structure $H^1_{\mathrm{dR}}(E_a)$ has a counterpart in the realm of p-adic Galois representations: the *étale cohomology group* $H^1_{\mathrm{et}}(E_a, \mathbb{Q}_p)$ which fits into an exact sequence

$$0 \longrightarrow H^1_{\mathrm{et}}(E, \mathbb{Q}_p) \longrightarrow H^1_{\mathrm{et}}(E_a, \mathbb{Q}_p) \longrightarrow \mathbb{Q}_p(-1) \longrightarrow 0.$$

Conjecture (Shafarevich, Tate)

If E is an elliptic curve, and ξ is a class in $\mathrm{Ext}^1_{Rep_{G_{\mathbb{Q}}}}(\mathbb{Q}_p(-1), H^1_{\mathrm{et}}(E, \mathbb{Q}_p))$ satisfying suitable explicit "local conditions", then ξ is proportional to the class of E_a, for some $a \in E(\mathbb{Q})$.

Conclusion

To construct points on elliptic curves, it "suffices" (modulo some deep conjectures!) to construct suitable

1. extensions of $\mathbb{C}(-1)$ by $H^1_{\mathrm{dR}}(E)$, in the category of *mixed Hodge structures*.
2. extensions of $\mathbb{Q}_p(-1)$ by $H^1_{\mathrm{et}}(E, \mathbb{Q}_p)$, in the category of continuous p-adic representations of $G_{\mathbb{Q}}$.

The first approach is good for practical numerical computations, while the second tends to be better for theoretical applications.

Conclusion

To construct points on elliptic curves, it "suffices" (modulo some deep conjectures!) to construct suitable

1. extensions of $\mathbb{C}(-1)$ by $H^1_{\mathrm{dR}}(E)$, in the category of *mixed Hodge structures*.
2. extensions of $\mathbb{Q}_p(-1)$ by $H^1_{\mathrm{et}}(E, \mathbb{Q}_p)$, in the category of continuous p-adic representations of $G_{\mathbb{Q}}$.

The first approach is good for practical numerical computations, while the second tends to be better for theoretical applications.

Conclusion

To construct points on elliptic curves, it "suffices" (modulo some deep conjectures!) to construct suitable

1. extensions of $\mathbb{C}(-1)$ by $H^1_{\mathrm{dR}}(E)$, in the category of *mixed Hodge structures*.
2. extensions of $\mathbb{Q}_p(-1)$ by $H^1_{\mathrm{et}}(E, \mathbb{Q}_p)$, in the category of continuous p-adic representations of $G_{\mathbb{Q}}$.

The first approach is good for practical numerical computations, while the second tends to be better for theoretical applications.

Conclusion

To construct points on elliptic curves, it "suffices" (modulo some deep conjectures!) to construct suitable

1. extensions of $\mathbb{C}(-1)$ by $H^1_{\mathrm{dR}}(E)$, in the category of *mixed Hodge structures*.
2. extensions of $\mathbb{Q}_p(-1)$ by $H^1_{\mathrm{et}}(E, \mathbb{Q}_p)$, in the category of continuous p-adic representations of $G_{\mathbb{Q}}$.

The first approach is good for practical numerical computations, while the second tends to be better for theoretical applications.

Modular curves

The Poincaré upper half-plane $\mathcal{H}$ is acted on discretely by

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z}) \text{ such that } N|c \right\}.$$

The algebraic curve $X_0(N)$ satisfying

$$X_0(N)(\mathbb{C}) = \Gamma_0(N)\backslash(\mathcal{H} \cup \mathbb{P}_1(\mathbb{Q})),$$

has a model over $\mathbb{Q}$, and is called the *modular curve of level N*.

Modular curves

The Poincaré upper half-plane $\mathcal{H}$ is acted on discretely by

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}_2(\mathbb{Z}) \text{ such that } N|c \right\}.$$

The algebraic curve $X_0(N)$ satisfying

$$X_0(N)(\mathbb{C}) = \Gamma_0(N)\backslash(\mathcal{H} \cup \mathbb{P}_1(\mathbb{Q})),$$

has a model over $\mathbb{Q}$, and is called the *modular curve of level N*.

Wiles' theorem, revisited

Theorem (Wiles)

The p-adic representation $H^1_{\text{et}}(E, \mathbb{Q}_p)$ is a constitutent of $H^1_{\text{et}}(X_0(N), \mathbb{Q}_p)$ for a suitable integer N (the conductor *of E).*

Corollary (Faltings)

There is a non-constant morphism $X_0(N) \longrightarrow E$ of curves over $\mathbb{Q}$.

These two theorems give us an extremely tight control on the arithmetic of the elliptic curve E.

Wiles' theorem, revisited

Theorem (Wiles)

The p-adic representation $H^1_{\text{et}}(E, \mathbb{Q}_p)$ is a constitutent of $H^1_{\text{et}}(X_0(N), \mathbb{Q}_p)$ for a suitable integer N (the conductor *of E).*

Corollary (Faltings)

There is a non-constant morphism $X_0(N) \longrightarrow E$ of curves over $\mathbb{Q}$.

These two theorems give us an extremely tight control on the arithmetic of the elliptic curve E.

Wiles' theorem, revisited

Theorem (Wiles)

The p-adic representation $H^1_{\text{et}}(E, \mathbb{Q}_p)$ is a constitutent of $H^1_{\text{et}}(X_0(N), \mathbb{Q}_p)$ for a suitable integer N (the conductor *of E).*

Corollary (Faltings)

There is a non-constant morphism $X_0(N) \longrightarrow E$ of curves over $\mathbb{Q}$.

These two theorems give us an extremely tight control on the arithmetic of the elliptic curve E.

Open modular curves

The modular curve $X_0(N)$ is equipped with a distinguished supply of algebraic points, arising from the *theory of complex multiplication*. The complement of any finite set of such points will be called an *open modular curve*.

Open modular curves

The modular curve $X_0(N)$ is equipped with a distinguished supply of algebraic points, arising from the *theory of complex multiplication*. The complement of any finite set of such points will be called an *open modular curve*.

Modularity of points on elliptic curves

A point $a \in E(\mathbb{Q})$ is said to be *modular* if $H^1(E_a)$ arises in $H^1(Y)$ for *some* open modular curve.

Theorem (Gross-Zagier)

If the L-function of E has a simple zero at $s = 1$, then any point in $E(\mathbb{Q})$ is modular in this sense.

Modularity of points on elliptic curves

A point $a \in E(\mathbb{Q})$ is said to be *modular* if $H^1(E_a)$ arises in $H^1(Y)$ for *some* open modular curve.

Theorem (Gross-Zagier)

If the L-function of E has a simple zero at $s = 1$, then any point in $E(\mathbb{Q})$ is modular in this sense.

Shimura varieties

There is a rich fauna of higher-dimensional generalisations of modular curves: the *Shimura varieties* which play a key role in the arithmetic theory of automorphic forms. An *open Shimura variety* is the complement of a Shimura subvariety.

Definition

Let E be an elliptic curve over a number field K. A point $a \in E(K)$ is *modular* if there is an (open) Shimura variety Y and an inclusion $H^1(E_a) \subset H^*(Y)(j)$. (In the category of mixed Hodge structures, or of p-adic Galois representations.)

Question: What pairs $(E_{/K}, a)$ are captured by constructions of this type?

This interesting question is largely open.

Shimura varieties

There is a rich fauna of higher-dimensional generalisations of modular curves: the *Shimura varieties* which play a key role in the arithmetic theory of automorphic forms. An *open Shimura variety* is the complement of a Shimura subvariety.

Definition

Let E be an elliptic curve over a number field K. A point $a \in E(K)$ is *modular* if there is an (open) Shimura variety Y and an inclusion $H^1(E_a) \subset H^*(Y)(j)$. (In the category of mixed Hodge structures, or of p-adic Galois representations.)

Question: What pairs $(E_{/K}, a)$ are captured by constructions of this type?

This interesting question is largely open.

Shimura varieties

There is a rich fauna of higher-dimensional generalisations of modular curves: the *Shimura varieties* which play a key role in the arithmetic theory of automorphic forms. An *open Shimura variety* is the complement of a Shimura subvariety.

Definition

Let E be an elliptic curve over a number field K. A point $a \in E(K)$ is *modular* if there is an (open) Shimura variety Y and an inclusion $H^1(E_a) \subset H^*(Y)(j)$. (In the category of mixed Hodge structures, or of p-adic Galois representations.)

Question: What pairs $(E_{/K}, a)$ are captured by constructions of this type?

This interesting question is largely open.

Shimura varieties

There is a rich fauna of higher-dimensional generalisations of modular curves: the *Shimura varieties* which play a key role in the arithmetic theory of automorphic forms. An *open Shimura variety* is the complement of a Shimura subvariety.

Definition

Let E be an elliptic curve over a number field K. A point $a \in E(K)$ is *modular* if there is an (open) Shimura variety Y and an inclusion $H^1(E_a) \subset H^*(Y)(j)$. (In the category of mixed Hodge structures, or of p-adic Galois representations.)

Question: What pairs $(E_{/K}, a)$ are captured by constructions of this type?

This interesting question is largely open.

Shimura varieties

There is a rich fauna of higher-dimensional generalisations of modular curves: the *Shimura varieties* which play a key role in the arithmetic theory of automorphic forms. An *open Shimura variety* is the complement of a Shimura subvariety.

Definition

Let E be an elliptic curve over a number field K. A point $a \in E(K)$ is *modular* if there is an (open) Shimura variety Y and an inclusion $H^1(E_a) \subset H^*(Y)(j)$. (In the category of mixed Hodge structures, or of p-adic Galois representations.)

Question: What pairs $(E_{/K}, a)$ are captured by constructions of this type?

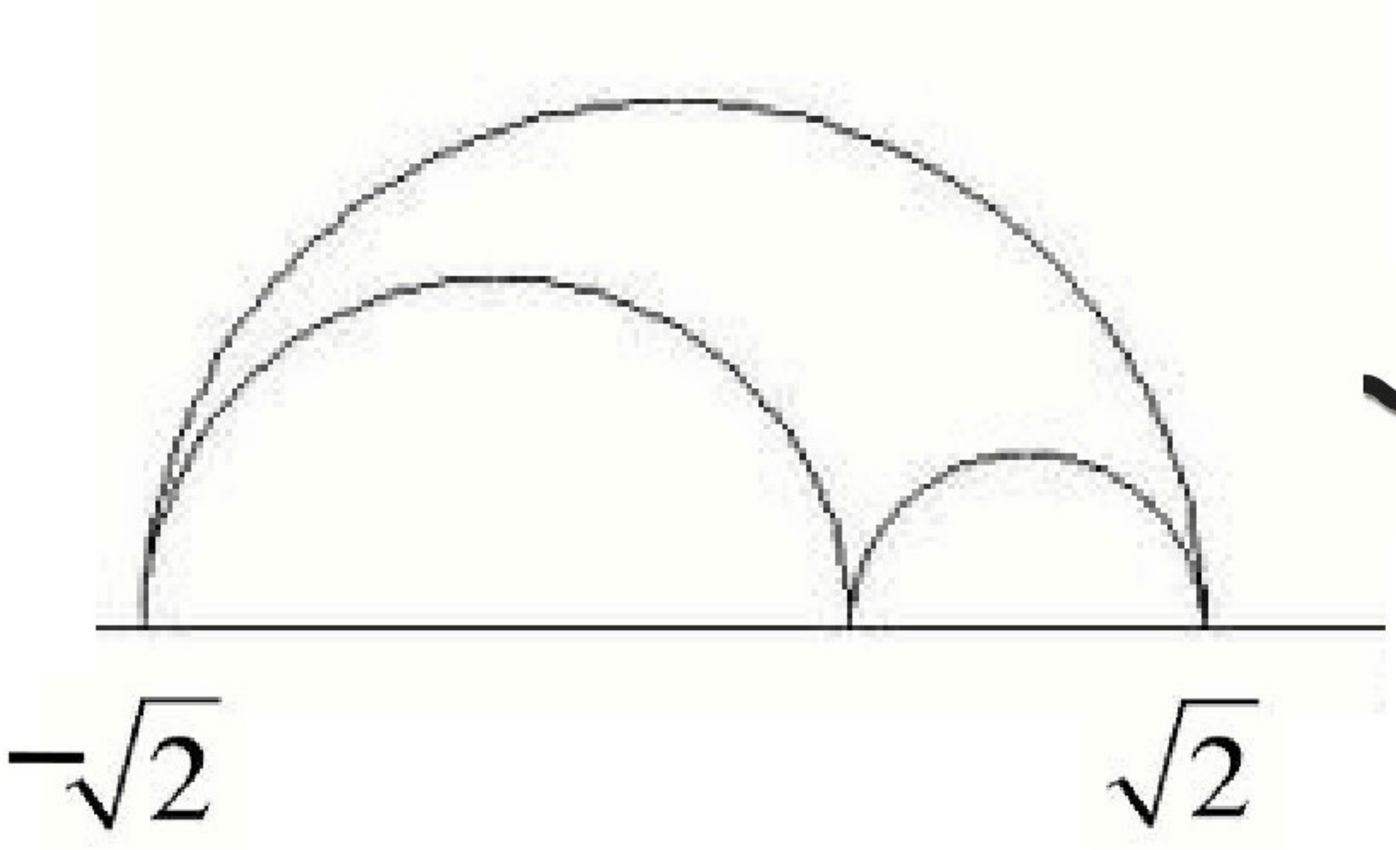
This interesting question is largely open.

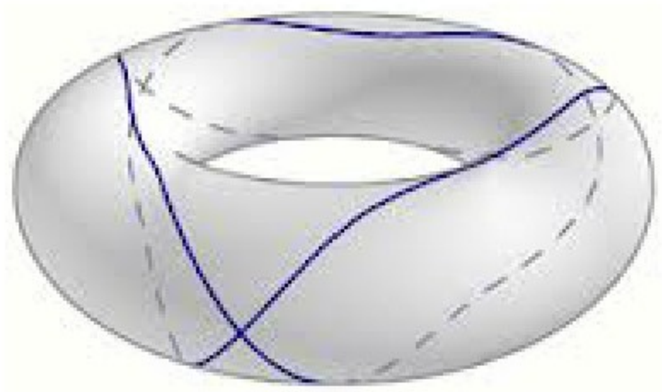
Stark-Heegner points

Shimura varieties are also equipped with a rich variety of distinguished *topological cycles* which do not have any a priori algebraic meaning.

Stark-Heegner points

Shimura varieties are also equipped with a rich variety of distinguished *topological cycles* which do not have any a priori algebraic meaning.





Stark-Heegner points

Nonetheless, such topological cycles can sometimes be used to construct explicit extensions of mixed Hodge structures (or p-adic variants thereof) which correspond, *conjecturally*, to global points on elliptic curves: the so-called *Stark-Heegner points*.

The phenomenon of Stark-Heegner points is quite mysterious and poorly understood — a better understanding of it would lead to fundamental insights into the arithmetic of elliptic curves, and to constructions of global points

1. defined over class fields of real quadratic fields;
2. defined over abelian extensions of certain non-CM fields;
3. on elliptic curves over imaginary quadratic fields.

Stark-Heegner points

Nonetheless, such topological cycles can sometimes be used to construct explicit extensions of mixed Hodge structures (or p-adic variants thereof) which correspond, *conjecturally*, to global points on elliptic curves: the so-called *Stark-Heegner points*.

The phenomenon of Stark-Heegner points is quite mysterious and poorly understood — a better understanding of it would lead to fundamental insights into the arithmetic of elliptic curves, and to constructions of global points

1. defined over class fields of real quadratic fields;
2. defined over abelian extensions of certain non-CM fields;
3. on elliptic curves over imaginary quadratic fields.

Stark-Heegner points

Nonetheless, such topological cycles can sometimes be used to construct explicit extensions of mixed Hodge structures (or p-adic variants thereof) which correspond, *conjecturally*, to global points on elliptic curves: the so-called *Stark-Heegner points*.

The phenomenon of Stark-Heegner points is quite mysterious and poorly understood — a better understanding of it would lead to fundamental insights into the arithmetic of elliptic curves, and to constructions of global points

1. defined over class fields of real quadratic fields;
2. defined over abelian extensions of certain non-CM fields;
3. on elliptic curves over imaginary quadratic fields.

Stark-Heegner points

Nonetheless, such topological cycles can sometimes be used to construct explicit extensions of mixed Hodge structures (or p-adic variants thereof) which correspond, *conjecturally*, to global points on elliptic curves: the so-called *Stark-Heegner points*.

The phenomenon of Stark-Heegner points is quite mysterious and poorly understood — a better understanding of it would lead to fundamental insights into the arithmetic of elliptic curves, and to constructions of global points

1. defined over class fields of real quadratic fields;
2. defined over abelian extensions of certain non-CM fields;
3. on elliptic curves over imaginary quadratic fields.

Stark-Heegner points

Nonetheless, such topological cycles can sometimes be used to construct explicit extensions of mixed Hodge structures (or p-adic variants thereof) which correspond, *conjecturally*, to global points on elliptic curves: the so-called *Stark-Heegner points*.

The phenomenon of Stark-Heegner points is quite mysterious and poorly understood — a better understanding of it would lead to fundamental insights into the arithmetic of elliptic curves, and to constructions of global points

1. defined over class fields of real quadratic fields;
2. defined over abelian extensions of certain non-CM fields;
3. on elliptic curves over imaginary quadratic fields.

Stark-Heegner points

Nonetheless, such topological cycles can sometimes be used to construct explicit extensions of mixed Hodge structures (or p-adic variants thereof) which correspond, *conjecturally*, to global points on elliptic curves: the so-called *Stark-Heegner points*.

The phenomenon of Stark-Heegner points is quite mysterious and poorly understood — a better understanding of it would lead to fundamental insights into the arithmetic of elliptic curves, and to constructions of global points

1. defined over class fields of real quadratic fields;
2. defined over abelian extensions of certain non-CM fields;
3. on elliptic curves over imaginary quadratic fields.

Stark-Heegner points

They have been intensely studied in the last years, both theoretically and experimentally, in Italy,

Massimo Bertolini

Matteo Longo

Marco Seveso

Stefano Vigni

Stark-Heegner points

In Spain,

Victor
Rotger

Xavier
Guitart

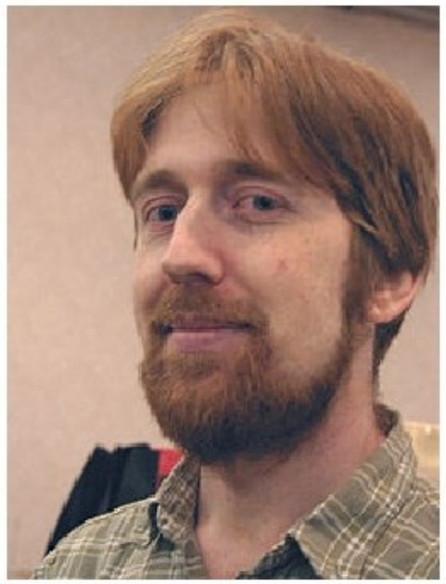
Marc
Masdeu

Stark-Heegner points

On the east coast,

Chung-Pang Mok

Robert Pollack



Adam Logan

Yu Zhao

Hugo Chapdelaine

Stark-Heegner points

.... and right here out West !

Matt Greenberg

Mak Trifkovic

A promising approach

One approach to understanding Stark-Heegner points is to try to construct the extension classes

$$\xi \in \mathrm{Ext}_{\mathrm{Rep}_{G_{\mathbb{Q}}}}(\mathbb{Q}_p(-1), H^1_{\mathrm{et}}(E, \mathbb{Q}_p))$$

that should arise from Stark-Heegner points, as *p-adic limits* of extension classes arising from a collection of open Shimura varieties.

A promising approach

Ongoing work—notably by Matt Greenberg and Marco Seveso—on p-adic L-functions for "Garrett Rankin triple products" offers hope that significant progress on these mysterious constructions will be achieved in the coming years.

Thank you for your attention.