

Fermat's Last Theorem

Lecture III

Nuno Freitas

nuno.freitas@icmat.es

Second Portuguese number theory meeting

4 – 8 Sep 2023

Motivation

Fermat's Last Theorem

The only solutions (a, b, c) to the equation

$$x^n + y^n + z^n = 0, \quad a, b, c \in \mathbb{Z}, \quad n \geq 3$$

satisfy $abc \neq 0$.

Theorem (Wiles, Taylor–Wiles)

All semistable elliptic curves over \mathbb{Q} are modular.

Wiles' theorem was later extended to all elliptic curves over \mathbb{Q} by the work of Breuil, Conrad, Diamond and Taylor.

A sketch of modularity

A quadratic example

Before discussing modularity of elliptic curves, which are cubic equations, we start with the simpler case of the quadratic equation

$$Q : x^2 = D \quad \text{with } D > 0 \text{ an odd integer.}$$

It makes sense to consider Q modulo different primes p :

$$\overline{Q} : x^2 = \overline{D} \quad \text{as an equation in } \mathbb{F}_p.$$

Denote by $\#\overline{Q}(\mathbb{F}_p)$ its number of solutions in \mathbb{F}_p and define

$$a_p(Q) := \#\overline{Q}(\mathbb{F}_p) - 1.$$

Observe that, for all primes $p \nmid D$, there are either 2 or 0 solutions, so in the previous definition we are subtract 1 which is the “expected” number of solutions.

The Legendre and Jacobi symbols

For an integer m and an odd prime p , the **Legendre symbol** is

$$\left(\frac{m}{p}\right) = \begin{cases} 1 & \text{if } p \nmid m \text{ and } m \text{ is a square modulo } p, \\ -1 & \text{if } p \nmid m \text{ and } m \text{ is not a square modulo } p, \\ 0 & \text{if } p \mid m. \end{cases}$$

For $m, n \in \mathbb{Z}$ with $n > 0$, the **Jacobi symbol** is given by

$$\left(\frac{m}{n}\right) = \left(\frac{m}{p_1}\right)^{e_1} \cdots \left(\frac{m}{p_k}\right)^{e_k},$$

where $n = p_1^{e_1} \cdots p_k^{e_k}$ is the prime factorization of n and on the right we have Legendre symbols.

Quadratic Reciprocity

The Jacobi symbol satisfies that

$$\left(\frac{m}{n}\right) = \left(\frac{m'}{n}\right) \quad \text{if } m \equiv m' \pmod{n}.$$

Moreover, it satisfies the following **very important** theorem in elementary number theory.

Theorem (Quadratic Reciprocity Law)

Let $m, n > 0$ be odd coprime integers. We have

$$\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2} \frac{n-1}{2}} \left(\frac{n}{m}\right).$$

A quadratic example

Reducing $Q : x^2 = D$ modulo different primes we obtained

$$\overline{Q} : x^2 = \overline{D} \quad \text{as an equation in } \mathbb{F}_p.$$

We denote by $\#\overline{Q}(\mathbb{F}_p)$ its number of solutions and defined

$$a_p(Q) := \#\overline{Q}(\mathbb{F}_p) - 1.$$

Therefore,

$$a_p(Q) = \left(\frac{D}{p} \right),$$

so by the Quadratic Reciprocity Law

$$a_p(Q) = (-1)^{\binom{D-1}{2} \binom{p-1}{2}} \left(\frac{p}{D} \right).$$

A quadratic example.

Suppose $q \equiv p \pmod{4D}$ is also prime. Then

$$q \equiv p \pmod{D} \quad \text{and} \quad \frac{p-1}{2} \equiv \frac{q-1}{2} \pmod{2}$$

therefore

$$a_q(Q) = (-1)^{\binom{D-1}{2}\binom{q-1}{2}} \left(\frac{q}{D}\right) = (-1)^{\binom{D-1}{2}\binom{p-1}{2}} \left(\frac{p}{D}\right) = a_p(Q)$$

so $a_p(Q)$ only depends on p modulo $4D$.

- ▶ This is remarkable!
- ▶ Usually, it is unclear one should expect any connection between the solutions of equations modulo different primes.
- ▶ Any formula giving information on solutions modulo different primes is referred to as a “reciprocity law”.
- ▶ Reciprocity laws give some coherence to certain sequences of apparently unrelated integers, e.g. the sequence $\{a_p(Q)\}$.

A quadratic example – a family of linear operators

A key insight towards modularity is to reinterpret the sequence $\{a_p(Q)\}$, as a **system of eigenvalues** of certain linear operators acting on a finite dimensional \mathbb{C} -vector space.

First we define $a_n(Q)$ for non-prime n multiplicatively

$$a_{n_1 n_2}(Q) := a_{n_1}(Q) a_{n_2}(Q),$$

so $a_n(Q)$ depends only on n modulo $4D$.

Let $N = 4D$ and define

$$V_N = \left\{ \text{functions } f : (\mathbb{Z}/N\mathbb{Z})^\times \rightarrow \mathbb{C} \right\},$$

which is a finite dimensional \mathbb{C} -vector space.

For each prime p , define a linear operator $T_p : V_N \rightarrow V_N$ as

$$T_p(f)(n) := \begin{cases} f(pn) & \text{if } p \nmid N \\ 0 & \text{else,} \end{cases}$$

where we consider pn after reduction modulo N .

A quadratic example – a family of linear operators

For each prime p , define a linear operator $T_p : V_N \rightarrow V_N$ as

$$T_p(f)(n) := \begin{cases} f(pn) & \text{if } p \nmid N \\ 0 & \text{else,} \end{cases}$$

where we consider pn after reduction modulo N .

The operators T_p commute with each other.

To the quadratic equation $Q : x^2 = D$ we can associate the function $f_Q \in V_N$, defined by

$$f_Q(n) := a_n(Q)$$

which is well defined because of the Quadratic Reciprocity Law!

Further, for each prime p and all $n \in (\mathbb{Z}/N\mathbb{Z})^\times$, we have

$$T_p(f_Q)(n) = f_Q(pn) = a_{pn}(Q) = a_p(Q)a_n(Q) = a_p(Q)f_Q(n),$$

that is,

$$T_p(f_Q) = a_p(Q)f_Q.$$

Summary of the quadratic example

- ▶ To the equation $Q : x^2 = D$ we can associate a function f_Q ;
- ▶ f_Q belongs to a finite dimensional \mathbb{C} -vector space;
- ▶ f_Q is a common eigenvector for all the linear operators T_p .
- ▶ The corresponding eigenvalues are the integers $a_p(Q)$ that can be computed by **counting points on curves**.
- ▶ We say that Q **arises** from f_Q .
- ▶ This is a consequence of the Quadratic Reciprocity Law, a deep classical result.

A classical motivation for modular forms

The partition function

For each $n \geq 0$, define the **partition function** $p(n)$ as

$$p(n) = \#\{\text{ways of representing } n \text{ as a sum of natural numbers}\}.$$

As a convention, $p(0) = 1$. Also, note that:

$$p(1) = 1$$

$$p(2) = 2 = \#\{1 + 1, 2\}$$

$$p(3) = 3 = \#\{1 + 1 + 1, 1 + 2, 3\}$$

$$p(4) = 5 = \#\{1 + 1 + 1 + 1, 1 + 1 + 2, 1 + 3, 2 + 2, 4\}$$

...

We package all these numbers together in the formal powers series:

$$P(q) = \sum_{n=0}^{\infty} p(n)q^n,$$

where we think of q as a formal variable.

The partition function

Lemma

$$P(q) = \sum_{n=0}^{\infty} p(n)q^n = \prod_{m=1}^{\infty} \frac{1}{1-q^m}.$$

In view of the lemma, a convenient way to study the partition function is through the following infinite product:

$$\Delta(q) = q \prod_{n=1}^{\infty} (1 - q^n)^{24}.$$

We have

$$\begin{aligned} \Delta(q) &= q \prod_{n=1}^{\infty} (1 - q^n)^{24} = \frac{q \prod_{n=1}^{\infty} (1 - q^n)^{25}}{\prod_{n=1}^{\infty} (1 - q^n)} \\ &= \left(\prod_{n=1}^{\infty} (1 - q^n)^{25} \right) \sum_{n=0}^{\infty} p(n)q^{n+1} = \sum_{n=1}^{\infty} \tau(n)q^n, \end{aligned}$$

where τ is the *Ramanujan τ -function*.

The Ramanujan τ -function

We defined *Ramanujan's tau* function via:

$$\Delta(q) = \sum_{n=1}^{\infty} \tau(n)q^n.$$

Theorem (Ramanujan)

For each $n \geq 1$, we have

$$\tau(n) \equiv \sum_{d|n} d^{11} \pmod{691}.$$

Conjecture (Ramanujan)

- (1) For all $m, n > 0$ coprime, we have $\tau(mn) = \tau(m)\tau(n)$
- (2) For all primes p , we have

$$\tau(p)\tau(p^n) = \tau(p^{n+1}) - p^{11}\tau(p^{n-1}).$$

Modular forms

The group $\Gamma_0(N)$

The **modular group** is

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z}) : \det \gamma = ad - bc = 1 \right\}.$$

There are modular forms associated with different subgroups Γ of the modular group. For **modularity of elliptic curves** we are interested in $\Gamma = \Gamma_0(N)$ where N is a positive integer.

More precisely,

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod{N} \right\}$$

which is a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ of finite index.

These groups act on $\mathcal{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$ via **fractional linear transformations**

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : \mathcal{H} \rightarrow \mathcal{H}, \quad z \mapsto \frac{az + b}{cz + d}.$$

Fundamental domains

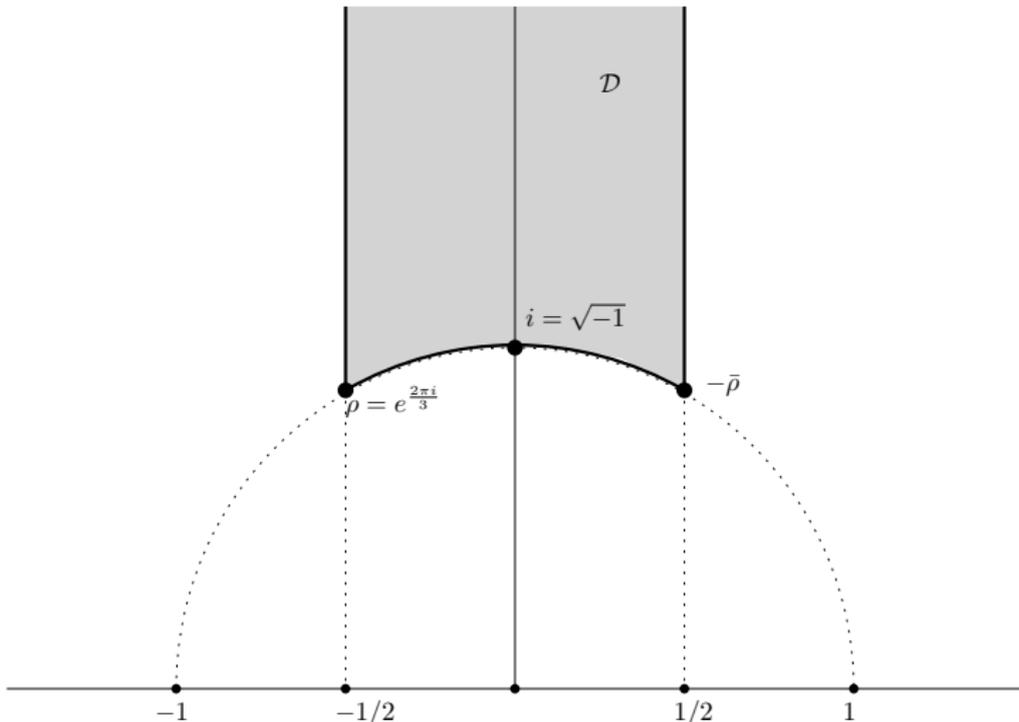


Figure: Fundamental domain for $SL_2(\mathbb{Z})$

Fundamental domains

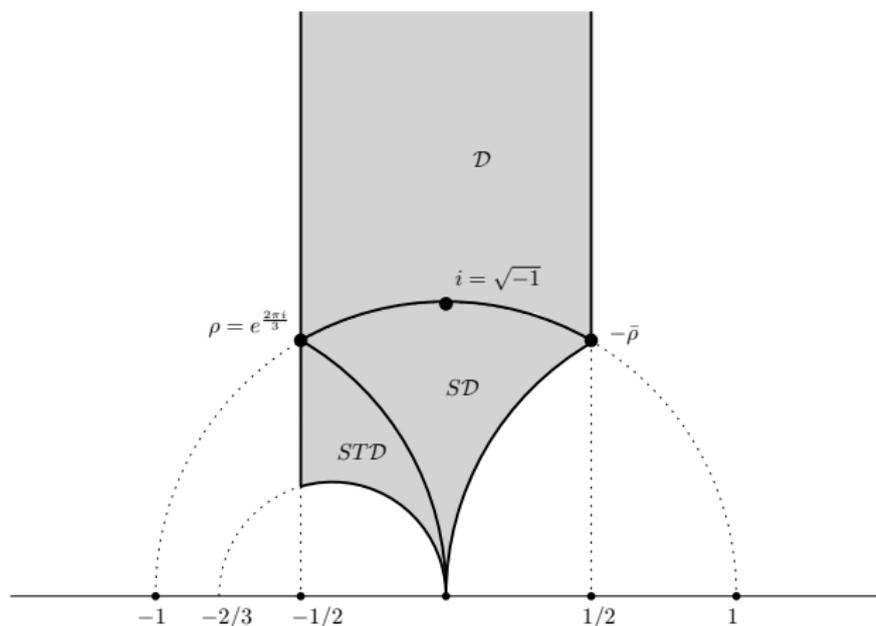
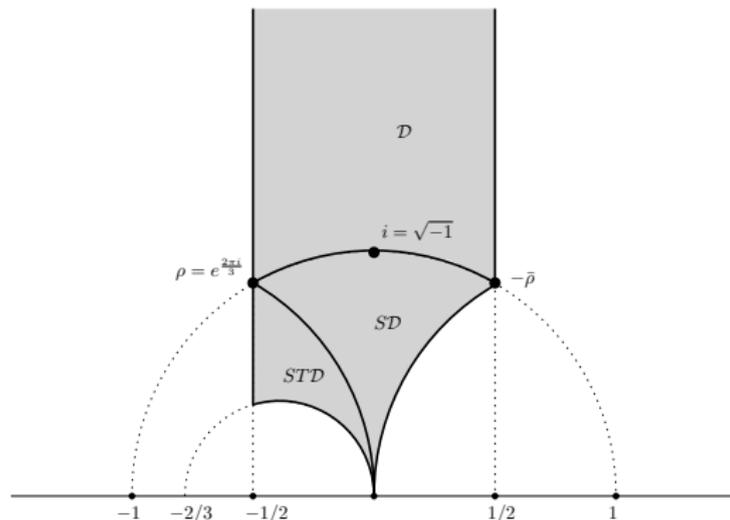


Figure: A fundamental domain for $\Gamma_0(2)$, where $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$

$$\Gamma_0(2) = \left\{ \gamma \in \mathrm{SL}_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{2} \right\}$$

Fundamental domains



- ▶ We see that ∞ and $z = (0, 0)$ are limit points for $\Gamma_0(2)$.
- ▶ In general, different subgroups $\Gamma_0(N) \subset \text{SL}_2(\mathbb{Z})$ give rise to different limit points, which we refer to as **cusps**.
- ▶ The quotient $Y_0(N) = \Gamma_0(N) \backslash \mathcal{H}$ has the structure of a non-compact Riemann surface. This has a standard compactification denoted $X_0(N)$ and the difference $X_0(N) - Y_0(N)$ is the finite set of points called the **cusps**.

Modular forms for $\Gamma_0(N)$

Note that $\Gamma_0(1) = \mathrm{SL}_2(\mathbb{Z})$.

Recall that $\mathcal{H} = \{z \in \mathbb{C} : \mathrm{Im}(z) > 0\}$.

Definition

A **modular form f of weight $k \geq 2$ for $\Gamma_0(N)$** is a function $f : \mathcal{H} \rightarrow \mathbb{C}$ that satisfies the following conditions :

- (i) f is holomorphic on \mathcal{H} ;
- (ii) for all $z \in \mathcal{H}$ and all $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$, we have

$$f(\gamma \cdot z) = f\left(\frac{az + b}{cz + d}\right) = (cz + d)^k f(z)$$

- (iii) f extends to a function that is holomorphic at the cusps.

The set of modular forms of weight k for $\Gamma_0(N)$ is denoted by $M_k(\Gamma_0(N))$. **It is a finite-dimensional \mathbb{C} -vector space.**

Modular forms for $\Gamma_0(N)$

- ▶ It follows from the defining properties that $f \in M_k(\Gamma_0(N))$ must have a Fourier expansion

$$f(z) = c_0 + \sum_{n \geq 1} c_n q^n \quad \text{where} \quad q(z) = \exp(2\pi iz).$$

- ▶ A **cusp form** of weight k for $\Gamma_0(N)$ is a $f \in M_k(\Gamma_0(N))$ that **vanishes** at all the cusps. This implies $c_0 = 0$.
- ▶ The cusp forms naturally form a subspace of $M_k(\Gamma_0(N))$ which we denote by $S_k(\Gamma_0(N))$.
- ▶ For each $n \geq 1$, there is a so-called **Hecke operator**

$$T_n : M_k(\Gamma_0(N)) \rightarrow M_k(\Gamma_0(N))$$

preserving the cuspidal subspace $S_k(\Gamma_0(N))$.

- ▶ The Hecke operators **commute** with each other.

Examples – the Eisenstein series for $SL_2(\mathbb{Z})$

Definition

Let $k \geq 4$ be an even integer. The **Eisenstein series of weight k for $SL_2(\mathbb{Z})$** is the function $G_k : \mathcal{H} \rightarrow \mathbb{C}$ given by

$$G_k(z) := \sum_{\substack{m,n \in \mathbb{Z} \\ (m,n) \neq (0,0)}} \frac{1}{(mz + n)^k}.$$

Theorem

Let $k \geq 4$ be even. The Eisenstein series G_k is a modular form of weight k and level $N = 1$. Moreover, its q -expansion is

$$G_k(z) = 2\zeta(k) + 2 \frac{(2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$$

where $\sigma_t(n) = \sum_{d|n} d^t$ is the **sum of t -powers divisors function**.

Examples – Eisenstein series and Δ function

By dividing $G_k(z)$ by its leading coefficient $2\zeta(k)$ we obtain the normalized Eisenstein series E_k . We can use it to construct modular forms with other weights !

Examples

- ▶ $E_4(z) = 1 + 240q + 2160q^2 + \dots$
- ▶ $E_6(z) = 1 - 504q - 16632q^2 - \dots$
- ▶ $E_4^3(z) = 1 + 720q + 179280q^2 + \dots$
- ▶ $E_6^2(z) = 1 - 1008q + 220752q^2 + \dots$
- ▶ A cuspform of weight $k = 12$:

$$\Delta(q) := \frac{E_4^3 - E_6^2}{1728} = q - 24q^2 + 252q^3 + \dots = \sum_{n \geq 1} \tau(n)q^n$$

Eigenforms

Definition

A modular form $f \in M_k(\mathrm{SL}_2(\mathbb{Z}))$ is called an **eigenform** if it is not identically zero and it is a common eigenvector for all the Hecke operators.

More precisely, for each $n \geq 1$, there is $\lambda_n \in \mathbb{C}$ such that

$$T_n f = \lambda_n f.$$

Further, we say that f is **normalized** if its q -expansion satisfies

$$a_1(f) = 1.$$

Eigenforms

Corollary

Let f, g be normalized eigenforms of weight k . If they have the same T_n -eigenvalues for all $n \geq 1$, then $f = g$.

Corollary

Let $f = \sum_{n \geq 0} a_n(f)q^n$ be a normalized eigenform of weight k .

(1) For all $m, n > 0$ coprime, we have

$$a_{nm}(f) = a_n(f)a_m(f).$$

(2) For all primes p , we have

$$a_p(f)a_{p^n}(f) = a_{p^{n+1}}(f) + p^{k-1}a_{p^{n-1}}(f).$$

Eigenforms

The space $S_{12}(\mathrm{SL}_2(\mathbb{Z}))$ has dimension one and contains

$$\Delta = \sum_{n \geq 1} \tau(n)q^n = q - 24q^2 + O(q^3),$$

Since T_n acts on $M_{12}(\mathrm{SL}_2(\mathbb{Z}))$ and preserves $S_{12}(\mathrm{SL}_2(\mathbb{Z}))$, we have that, for all $n \geq 1$,

$$T_n \Delta = \lambda_n \Delta \quad \text{for some } \lambda_n \in \mathbb{C},$$

hence Δ is a normalized eigenform. The corollary now yields

$$\tau(mn) = \tau(m)\tau(n)$$

for $m, n > 0$ coprime and, for all primes p ,

$$\tau(p)\tau(p^n) = \tau(p^{n+1}) - p^{11}\tau(p^{n-1})$$

as conjectured by Ramanujan.

Modularity of elliptic curves

Modularity of elliptic curves

- ▶ Let E/\mathbb{Q} be an elliptic curve of conductor N_E .
- ▶ For each prime p , there is a so-called **Hecke operator**

$$T_p : M_2(\Gamma_0(N_E)) \rightarrow M_2(\Gamma_0(N_E))$$

preserving the cuspidal subspace $S_2(\Gamma_0(N_E))$.

- ▶ The Hecke operators commute with each other.
- ▶ We say that E is **modular** if there exists some modular form $f_E \in S_2(N_E)$ such that f_E is a simultaneous eigenvector for all the Hecke operators T_p and

$$T_p(f_E) = a_p(E)f_E.$$

In this case, we say that E is **modular corresponding to the modular form** f_E or simply that E **'arises'** from f_E .

- ▶ Note the eigenvalues are the integers $a_p(E)$ which can be computed by **counting points on curves**.

Modularity of elliptic curves

We can now state the **modularity theorem**.

Theorem (Wiles, Breuil–Conrad–Diamond–Taylor)

Let E/\mathbb{Q} be an elliptic curve with conductor N_E .

There exists a cuspidal form $f \in S_2(\Gamma_0(N_E))$ that is normalized, an eigenvector for all the Hecke operators, and its q -expansion

$$f(z) = 1 + \sum_{n \geq 2} a_n(f)q^n$$

satisfies $a_n(f) \in \mathbb{Q}$ and

$$a_p(f) = a_p(E) \text{ for all } p \nmid N_E.$$

Modularity of elliptic curves

Example

The elliptic curve over \mathbb{Q} with the smallest conductor is

$$E : y^2 + y = x^3 - x^2$$

and it has conductor $N_E = 11$. Using a dimension formula or/and an algorithm to compute modular forms it follows there exists exactly one cuspform of weight 2 for $\Gamma_0(11)$, namely

$$q - 2q^2 - q^3 + 2q^4 + q^5 + 2q^6 - 2q^7 - 2q^9 + O(q^{10}).$$

Therefore this is the form attached to E/\mathbb{Q} by the modularity theorem.

L -functions attached to eigenforms

Let $f \in S_2(\Gamma_0(N))$ be a normalized eigenfunction for the Hecke operators with the q -expansion at infinity given by

$$f(z) = \sum_{n \geq 1} a_n(f) q^n.$$

The L -function attached to f is

$$L(f, s) = \sum_{n \geq 1} \frac{a_n(f)}{n^s}.$$

It is holomorphic on the right half plane $\operatorname{Re}(s) > 2$.

Moreover, $L(f, s)$ extends analytically to all of \mathbb{C} and satisfies a functional equation relating $L(f, s)$ and $L(f, 2 - s)$.

Modularity and L -functions

We can now give another (but equivalent) formulation of the modularity theorem.

Theorem (Modularity theorem)

Let E/\mathbb{Q} be an elliptic curve with conductor N_E . There exists a normalized cuspform $f \in S_2(\Gamma_0(N_E))$ that is an eigenvector for all the Hecke operators and satisfies

$$L(E, s) = L(f, s).$$

- ▶ This is an incredibly deep result.
- ▶ One of its most important consequences is that L -functions of elliptic curves over \mathbb{Q} admit an analytic continuation to all \mathbb{C} and satisfy a functional equation relating $L(E, s)$ and $L(E, 2 - s)$.
- ▶ This is not at all obvious, and the modularity theorem is currently the only known way to prove it.

Representations attached to eigenforms

Galois representations attached to eigenforms

Let f be a cuspidal form.

Denote by $\mathbb{Q}_f = \mathbb{Q}(\{a_p(f)\})$ the **coefficient field of f** .

Fact: If f is a normalized eigenform then $[\mathbb{Q}_f : \mathbb{Q}]$ is finite.

Theorem

Let $f \in \mathcal{S}_k(\Gamma_0(N))$ be a normalized eigenform. Let p be a prime.

For each prime ideal $\mathfrak{p} \mid p$ in \mathbb{Q}_f there is an **irreducible** 2-dimensional Galois representation

$$\rho_{f,\mathfrak{p}} : G_{\mathbb{Q}} \rightarrow \mathrm{GL}_2(\mathbb{Q}_{f,\mathfrak{p}}).$$

This representation is unramified at every prime $\ell \nmid pN$.

Moreover, for each $\ell \nmid pN$ the matrix $\rho_{f,\mathfrak{p}}(\mathrm{Frob}_{\ell})$ satisfies

$$x^2 - a_{\ell}(f)x + \ell^{k-1} = 0.$$

Galois representations attached to eigenforms

We can give yet another formulation of the modularity theorem.

Theorem (Modularity theorem)

Let E/\mathbb{Q} be an elliptic curve with conductor N_E .

Then E is modular of level N_E .

More precisely, there is a normalized eigenform $f_E \in \mathcal{S}_2(\Gamma_0(N_E))$ satisfying $\mathbb{Q}_f = \mathbb{Q}$ and such that

$$\rho_{E,p} \simeq \rho_{f_E,p} \quad \text{for all primes } p.$$

In particular, $a_\ell(f_E) = a_\ell(E)$ for all primes $\ell \nmid N_E$.

In fact, it suffices to have $\rho_{E,p} \simeq \rho_{f_E,p}$ for one prime p .

Residual modularity

Definition

Let $f \in S_2(\Gamma_0(N))$ be an eigenform, and $\mathfrak{p} \mid p$ in \mathbb{Q}_f .

We define the **mod \mathfrak{p} representation attached to f** as

$$\bar{\rho}_{f,\mathfrak{p}} := \rho_{f,\mathfrak{p}} \pmod{\mathfrak{p}}$$

which is well defined up to semi-simplification.

Definition

Let E/\mathbb{Q} be an elliptic curve. We say the representation $\bar{\rho}_{E,p}$ is **modular of level N** if for some eigenform f we have

$$\bar{\rho}_{E,p} \simeq \bar{\rho}_{f,\mathfrak{p}}.$$

In particular, for all prime $\ell \nmid N_E$, we have $a_\ell(E) \equiv a_\ell(f) \pmod{\mathfrak{p}}$

Corollary of modularity theorem

Let E/\mathbb{Q} be an elliptic curve. Then $\bar{\rho}_{E,p}$ is modular of level N_E .

Level lowering

Let E/\mathbb{Q} be an elliptic curve with conductor N_E .

Suppose there is an eigenform $g \in S_2(\Gamma_0(M))$ where the level M strictly divides N_E , and a prime $\mathfrak{P} \mid p$ in \mathbb{Q}_g such that

$$\bar{\rho}_{E,p} \simeq \bar{\rho}_{f_E,p} \simeq \bar{\rho}_{g,\mathfrak{P}}.$$

We call this **level lowering mod p** .

For example, take the curves

$$E : y^2 = x^3 - x^2 - 77x + 330, \quad F : y^2 = x^3 + x^2 + 3x - 1$$

$$N_E = 132 = 2^2 \cdot 3 \cdot 11, \quad \Delta_E = 2^4 3^{10} 11, \quad N_F = 44 = 2^2 \cdot 11$$

l	2	3	5	7	11	13	17	19
$a_l(E)$	0	-1	2	2	-1	6	-4	-2
$a_l(F)$	0	1	-3	2	-1	-4	6	8

We have $a_l(E) \equiv a_l(F) \pmod{5}$.

Level lowering

Theorem (Ribet)

Let E/\mathbb{Q} be an elliptic curve with minimal discriminant Δ and conductor N_E . Let $p \geq 3$ be a prime. Let also

$$N_p = \frac{N}{M_p}, \quad \text{where} \quad M_p = \prod_{\substack{\ell \parallel N, \\ p \mid v_\ell(\Delta)}} \ell.$$

Suppose that

- (i) the curve E is modular and
- (ii) the mod p representation $\bar{\rho}_{E,p}$ is irreducible.

Then $\bar{\rho}_{E,p} \simeq \bar{\rho}_{g,\mathfrak{p}}$ for some eigenform g of weight 2 and level N_p and a prime ideal $\mathfrak{p} \mid p$ in \mathbb{Q}_g .

Fermat's Last Theorem

Back to our motivation

Fermat's Last Theorem

The only solutions (a, b, c) to the equation

$$x^n + y^n + z^n = 0, \quad a, b, c \in \mathbb{Z}, \quad n \geq 3$$

satisfy $abc = 0$.

Theorem (Wiles, Taylor–Wiles)

All semistable (i.e. with squarefree conductor) elliptic curves over \mathbb{Q} are modular.

Observation:

- ▶ It is enough to prove FLT for $n = p$ a prime and $n = 4$;
- ▶ The cases $n = 3, 4$ were established by Euler and Fermat.

Proof of FLT:

Suppose that $a, b, c \in \mathbb{Z}$ and $p \geq 5$ a prime satisfy

$$a^p + b^p + c^p = 0, \quad abc \neq 0, \quad \gcd(a, b, c) = 1.$$

Following Frey, we define

$$E : y^2 = x(x - a^p)(x + b^p),$$

$$\Delta_E = 16a^{2p}b^{2p}(a^p + b^p)^2 = 16a^{2p}b^{2p}c^{2p} \neq 0.$$

Note: we can assume $a \equiv -1 \pmod{4}$ and $2 \mid b$.

From Tate's algorithm we get

$$N_E = 2 \cdot \prod_{\substack{\ell \mid abc \\ \ell \neq 2}} \ell.$$

By Wiles E is **modular**, then $\bar{\rho}_{E,p}$ is modular of level N_E .

Proof of FLT:

To apply Ribet's theorem, we need to compute

$$N_p = \frac{N_E}{M_p}, \quad M_p = \prod_{\substack{\ell | N_E \\ p | v_\ell(\Delta)}} \ell.$$

Recall that

$$\Delta = 16a^{2p}b^{2p}c^{2p}, \quad N_E = 2 \cdot \prod_{\substack{\ell | abc \\ \ell \neq 2}} \ell.$$

- ▶ Then $N_p = 2$;
- ▶ We already know $\bar{\rho}_{E,p}$ is modular of level N_E ;
- ▶ By **Mazur's irreducibility theorem** we conclude that $\bar{\rho}_{E,p}$ is irreducible;
- ▶ By **Ribet's level lowering theorem** we have that $\bar{\rho}_{E,p}$ is modular of level $N_p = 2$ (and weight 2).
- ▶ **;; There are no eigenforms of weight 2 and level 2!!** □

THANK YOU FOR COMING!