

Uniwersytet Warszawski
Wydział Matematyki, Informatyki i Mechaniki

Przemysław Chojecki

Nr albumu: 262926

On the modularity of elliptic curves

Praca licencjacka
na kierunku MATEMATYKA

Praca wykonana pod kierunkiem
dra hab. Adriana Langer
Instytut Matematyki

Czerwiec 2009

Oświadczenie kierującego pracą

Potwierdzam, że niniejsza praca została przygotowana pod moim kierunkiem i kwalifikuje się do przedstawienia jej w postępowaniu o nadanie tytułu zawodowego.

Data

Podpis kierującego pracą

Oświadczenie autora (autorów) pracy

Świadom odpowiedzialności prawnej oświadczam, że niniejsza praca dyplomowa została napisana przeze mnie samodzielnie i nie zawiera treści uzyskanych w sposób niezgodny z obowiązującymi przepisami.

Oświadczam również, że przedstawiona praca nie była wcześniej przedmiotem procedur związanych z uzyskaniem tytułu zawodowego w wyższej uczelni.

Oświadczam ponadto, że niniejsza wersja pracy jest identyczna z załączoną wersją elektroniczną.

Data

Podpis autora (autorów) pracy

Streszczenie

Praca ta jest przeglądem podstawowych definicji i twierdzeń, które są potrzebne do zrozumienia wyniku znanego obecnie jako twierdzenie o modularności. Szczególny przypadek tego twierdzenia, wystarczający do otrzymania Wielkiego Twierdzenia Fermata jako wniosku, został udowodniony w 1995 roku przez Andrew Wilesa (z pomocą Richarda Taylora), a w całej ogólności w 2000 roku przez Breuila, Conrada, Diamonda i Taylora. Dawniej twierdzenie o modularności było znane jako hipoteza Taniyamy-Shimury-Weila.

In this work I make a survey of basic definitions and theorems needed to understand a result called the Modularity Theorem. It was proved in '95 by Andrew Wiles (with a help of Richard Taylor) in the case when an elliptic curve in question is semistable and later in '00, it was proved in full generality by Breuil-Conrad-Diamond-Taylor. The statement of the theorem was known as the Taniyama-Shimura-Weil conjecture.

Słowa kluczowe

modular form, Galois representation, elliptic curve

Dziedzina pracy (kody wg programu Socrates-Erasmus)

11.1 Matematyka

Klasyfikacja tematyczna

11F11 Modular forms, one variable

Tytuł pracy w języku angielskim

On the modularity of elliptic curves

Table of contents

- Introduction
- Modular forms
- Modular curves
- Elliptic curves
- Geometric point of view
- Hecke operators
- Petersson inner product
- Oldforms and Newforms
- L-functions
- Jacobians and abelian varieties
- Galois representations
- Modularity
- Serres conjecture
- Examples
- Bibliography

Introduction

As a conjecture, the Modularity Theorem appeared around 1955 formulated by Yutaka Taniyama. Later it was reworked by Goro Shimura who gave it the correct wording, and popularized by Andre Weil who rediscovered it in 1967.

It was Gerhard Frey who in the 80s made a remark that the Taniyama-Shimura-Weil conjecture actually implies Fermat's Last Theorem. If FLT were false, it would give an elliptic curve which violate the Modularity Theorem.

After years of struggle, Andrew Wiles managed to prove the Modularity Theorem when an elliptic case in question is semistable. The proof was announced in 1993, but it was found to be flawed. After a help of Richard Taylor, the correct proof appeared in 1994 and it was published in 1995 (see [W], [TW]). A few years later Breuil, Conrad, Diamond and Taylor proved the Modularity Theorem in full generality (see [BCDT]).

The Taniyama-Shimura-Weil conjecture can be thought as a special case of Serre's conjecture which was probably formulated in the 70s. Extending results of Wiles and others, Khare with a help of Wintenberger proved Serre's conjecture in 2006 (see [KW1], [KW2]).

The work which I present here, is a survey of basic definitions and theorems around the Modularity Theorem. In exposition, I have followed mostly the beautiful book of Diamond and Shurman "A first course in the modular forms". I do not include any proofs as they are to be found in the afore-mentioned book. I had rather tried to expose the crucial material in as short a form as possible and make a guide through [DS].

Modular forms

$$\text{Let } \Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : a \equiv d \equiv 1 \pmod{N}, b \equiv c \equiv 0 \pmod{N} \right\}.$$

A subgroup Γ of $SL_2(\mathbb{Z})$ is called a **congruence subgroup** if $\Gamma(N) \subset \Gamma$ for some $N \in \mathbb{Z}^+$, in which case Γ is called a congruence subgroup of level N .

The most important examples of congruence subgroups are:

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : c \equiv 0 \pmod{N} \right\}$$

and

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : a \equiv d \equiv 1 \pmod{N}, c \equiv 0 \pmod{N} \right\}.$$

Let $\mathbb{H} = \{z \in \mathbb{C} : \text{Im}(z) > 0\}$. Observe that $SL_2(\mathbb{Z})$ acts on \mathbb{H} by $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot z = \frac{az+b}{cz+d}$.

For $k \in \mathbb{Z}$, $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$ and $f : \mathbb{H} \rightarrow \mathbb{C}$ we define $f[\gamma]_k$ by the formula

$$f[\gamma]_k(z) = \frac{1}{(cz+d)^k} f\left(\frac{az+b}{cz+d}\right).$$

Definition 1. Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$ and let k be a positive integer. A function $f : \mathbb{H} \rightarrow \mathbb{C}$ is called a **modular form of weight k with respect to Γ** if the following conditions are satisfied:

1. f is holomorphic,
2. $f[\gamma]_k = f$ for all $\gamma \in \Gamma$,
3. for every $\gamma \in SL_2(\mathbb{Z})$ we have $f[\gamma]_k(z) = \sum_{n=0}^{\infty} a(\gamma)_n e^{nz/N(\gamma)}$ for some $a(\gamma)_n \in \mathbb{C}$ and $N(\gamma) \in \mathbb{Z}^+$.

If in condition 3, $a(\gamma)_0 = 0$ for every $\gamma \in SL_2(\mathbb{Z})$ then f is called a **cuspidal form**.

Example 1. The basic example of a modular form of weight k for $SL_2(\mathbb{Z})$ is the Eisenstein series $G_k(z) = \sum_{(m,n) \in \mathbb{Z}^2 \setminus (0,0)} \frac{1}{(mz+n)^{2k}}$.

We will denote by $M_k(\Gamma)$ modular forms of weight k with respect to Γ and by $S_k(\Gamma)$ cuspidal forms of weight k with respect to Γ .

Modular curves

Let Γ be a congruence subgroup for $SL_2(\mathbb{Z})$ and define $\mathbb{H}^* = \mathbb{H} \cup \mathbb{Q} \cup \{\infty\}$ (where \mathbb{Q} are rational numbers). A **modular curve** is a curve of the form $X(\Gamma) = \Gamma \backslash \mathbb{H}^*$. The points $\Gamma \cdot s$ in $\Gamma \backslash \mathbb{Q} \cup \{\infty\}$ are called **cusps** of $X(\Gamma)$. It can be proved that each modular curve has only a finite number of cusps (2.4.1 in [DS]).

To put a topology on the curve $X(\Gamma)$, start by taking $N_M = \{z \in \mathbb{H} : \text{Im}(z) > M\}$ and take topology on \mathbb{H}^* with usual open sets in \mathbb{H} plus the sets $\alpha(N_M \cup \{\infty\})$ ($M > 0, \alpha \in SL_2(\mathbb{Z})$) as a base of neighborhoods of the cusps. Now, give $X(\Gamma)$ quotient topology.

It can be proved that with this topology $X(\Gamma)$ is a compact, connected Riemann surface (see 2.4.2 in [DS]).

We use notation $X_0(N), X_1(N)$ to denote $X(\Gamma_0(N)), X(\Gamma_1(N))$, respectively.

Elliptic curves

A complex **elliptic curve** is a smooth, projective curve of genus 1 defined over complex numbers. It can be shown that an elliptic curve is a set of complex solutions of an equation of the form $y^2 = ax^3 + bx + c$ where $a, b, c \in \mathbb{C}$ (see IV.4.6 in [Har] for details). Each elliptic curve has a structure of an abelian group.

A (1-dimensional) **complex torus** is a complex manifold of the form \mathbb{C}/Λ where Λ is a lattice in \mathbb{C} (a set of the form $a\mathbb{Z} + b\mathbb{Z}$ for some $a, b \in \mathbb{C}$ linearly independent over \mathbb{Z}).

With every complex torus we can associate Weierstrass function

$$\wp_\Lambda(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda, \omega \neq 0} \left(\frac{1}{(z - \omega)^2} + \frac{1}{\omega^2} \right).$$

If $G_k = \sum_{\omega \in \Lambda, \omega \neq 0} \frac{1}{\omega^{2k}}$ is the Eisenstein series and $g_2(\Lambda) = 60G_2(\Lambda)$, $g_3(\Lambda) = 140G_3(\Lambda)$, then one can prove that

$$(\wp'_\Lambda(z))^2 = 4(\wp_\Lambda(z))^3 - g_2(\Lambda)\wp_\Lambda(z) - g_3(\Lambda).$$

Hence we have an isomorphism between \mathbb{C}/Λ and the curve $E := (y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda))$ given by $z \mapsto (\wp_\Lambda(z), \wp'_\Lambda(z))$.

This shows that complex elliptic curves and 1-dimensional complex tori are the same thing.

By changing the coordinate system an elliptic curve can be put in the form $y^2 = x^3 + Ax + B$ and then we can define its ***j*-invariant** as

$$j(E) = \frac{1728 \cdot 4A^3}{4A^3 + 27B^2}.$$

For the notion of a **conductor** of an elliptic curve we refer to IV.10 in [Silv2]. This will be used only once to state one of the versions of the Modularity Theorem.

If E is an elliptic curve, let $E[n]$ denote a subgroup of its n -torsion points that is such points $P \in E$ that $nP = 0$. The ***l*-adic Tate module** of E is defined by setting $T_l(E) = \varprojlim E[l^n]$. It can be proved that $T_l(E)$ is isomorphic to $\mathbb{Z}_l \times \mathbb{Z}_l$, where \mathbb{Z}_l denotes l -adic integers (see III.7 of [Silv1]).

When E is defined over \mathbb{Q} (which is equivalent to $j(E) \in \mathbb{Q}$) we have an action of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ on each $E[l^n]$ and hence also on $T_l(E)$. This gives a representation $\rho_{E,l} : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow Aut(T_l(E))$. After choosing a \mathbb{Z}_l -basis for $T_l(E)$ and using the inclusion $\mathbb{Z}_l \subset \mathbb{Q}_l$ we obtain a representation $\rho_{E,l} : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow GL_2(\mathbb{Q}_l)$.

Now, we define an L -function associated with an elliptic curve E over \mathbb{Q} . Let $a_p(E) = p+1 - |\overline{E}(\mathbb{F}_p)|$ where \overline{E} is a reduction of E at p . We can extend it to $a_{p^e}(E) = p^e+1 - |\overline{E}(\mathbb{F}_{p^e})|$ and then to all k by demanding $a_{mn}(E) = a_m(E)a_n(E)$ for $(m, n) = 1$. Then the L -function associated to E is

$$L(s, E) = \sum_{n=1}^{\infty} a_n(E)n^{-s}.$$

See also 8.8 of [DS] or II.10 of [Silv2].

Geometric point of view

Observe that a modular form f of weight k with respect to Γ gives rise to a section of some line bundle on the modular curve $X(\Gamma)$. More precisely, the tensor $f(z)(dz)^{\otimes k/2}$ (k - even) has the property $f[\gamma]_k = f$ for all $\gamma \in \Gamma$ so it gives rise to a section of $\omega_{X(\Gamma)}^{\otimes k/2}$.

Later, we will use the fact that $S_2(\Gamma)$ is isomorphic to $\Omega_{hol}^1(X(\Gamma))$ via the map $f \mapsto f(z)dz$ (see 3.3 of [DS]).

More generally, from the geometric point of view, a modular form of weight k for $\Gamma_1(N)$ is a law which to every elliptic curve E with an inclusion $\alpha : \mu_N \hookrightarrow E$ associates a section of $\omega_E^{\otimes k}$.

Here μ_N is a group scheme of N -roots of unity, an elliptic curve E is understood as a proper smooth curve $\pi : E \rightarrow S$ relative to some scheme S , that is, geometrical fibers of π are elliptic curves and there exists a section $e : S \rightarrow E$ of π .

For more information on this see [Del-Se] or [Cais].

By using geometrical interpretation and standard facts about divisors (like the Riemann-Roch theorem) one can compute the dimension of the space of modular forms ($M_k(\Gamma)$) and of the space of cusp forms ($S_k(\Gamma)$). See chapter 3 of [DS].

Hecke operators

We will define operators on $M_k(\Gamma_1)$.

For $n \in (\mathbb{Z}/N\mathbb{Z})^*$ let us define a **diamond operator** $\langle n \rangle : M_k(\Gamma_1) \rightarrow M_k(\Gamma_1)$ given by $\langle n \rangle f = f[\alpha]_k$ for any $\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$ with $d \equiv n \pmod{N}$. Observe that this is well-defined. Define $\langle n \rangle$ for all n by setting $\langle n \rangle = \langle n \pmod{N} \rangle$ if $(n, N) = 1$ and $\langle n \rangle = 0$ otherwise.

For a prime number p let us define the p -th **Hecke operator** $T_p : M_k(\Gamma_1) \rightarrow M_k(\Gamma_1)$ by

$$T_p f = \begin{cases} \sum_{j=0}^{p-1} f \left[\begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix} \right]_k & \text{if } p|N, \\ \sum_{j=0}^{p-1} f \left[\begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix} \right]_k + f \left[\begin{pmatrix} m & n \\ N & p \end{pmatrix} \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \right]_k & \text{if } p \nmid N, \end{cases}$$

where m, n are any integers satisfying $mp - nN = 1$.

We define T_n for arbitrary n inductively. Set $T_1 = id$. We have defined T_p for primes p and we define now:

$$T_{p^r} = T_p T_{p^{r-1}} - p^{k-1} \langle p \rangle T_{p^{r-2}}$$

for $r \geq 2$.

After checking that $T_{p^r} T_{q^s} = T_{q^s} T_{p^r}$ for arbitrary primes p, q we can set:

$$T_n = \prod T_{p_i^{e_i}}$$

for $n = \prod p_i^{e_i}$.

The **Hecke algebra** over \mathbb{Z} is a subalgebra of the algebra of endomorphisms of $S_2(\Gamma_1(N))$ generated over \mathbb{Z} by the Hecke operators, that is:

$$T_{\mathbb{Z}} = \mathbb{Z}[\{T_n, \langle n \rangle : n \in \mathbb{Z}^+\}].$$

We also set $T_{\mathbb{C}} = \mathbb{C}[\{T_n, \langle n \rangle : n \in \mathbb{Z}^+\}]$.

Petersson inner product

A fundamental domain of \mathbb{H}^* under the action of $SL_2(\mathbb{Z})$ is $D^* = \{z \in \mathbb{H} : \operatorname{Re}(z) \leq 1/2, |z| \geq 1\} \cup \{\infty\}$.

Let $d\mu(z) = \frac{dx dy}{y^2}$ (where $z = x + iy \in \mathbb{H}$) be the hyperbolic measure. Observe that this measure is invariant under the action of $SL_2(\mathbb{Z})$.

For any continuous, bounded function $\phi : \mathbb{H} \rightarrow \mathbb{C}$ and any $\alpha \in SL_2(\mathbb{Z})$, the integral $\int_{D^*} \phi(\alpha(z)) d\mu(z)$ converges.

Let Γ be a congruence subgroup of $SL_2(\mathbb{Z})$ and let $\{\alpha_j\} \subset SL_2(\mathbb{Z})$ represent the coset space $\{\pm I\}\Gamma \backslash SL_2(\mathbb{Z})$. If ϕ is Γ -invariant then $\sum_j \int_{\alpha_j(D^*)} \phi(\alpha(z)) d\mu(z)$ is independent of the choice of coset representatives α_j . We write

$$\int_{X(\Gamma)} \phi(z) d\mu(z) = \sum_j \int_{\alpha_j(D^*)} \phi(\alpha(z)) d\mu(z).$$

Let $V_\Gamma = \int_{X(\Gamma)} d\mu(z)$ be the volume of $X(\Gamma)$. One can check that

$$\phi(z) = f(z) \overline{g(z)} (\operatorname{Im}(z))^k$$

for $f, g \in S_k(\Gamma)$ is Γ -invariant and bounded (see 5.4 of [DS]). This allows us to define the **Petersson inner product** as:

$$\langle f, g \rangle_\Gamma = \frac{1}{V_\Gamma} \int_{X(\Gamma)} f(z) \overline{g(z)} (\operatorname{Im}(z))^k d\mu(z).$$

Oldforms and Newforms

Let $\alpha_d = \begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix}$. For each divisor d of N we define the map

$$i_d : (S_k(\Gamma_1(Nd^{-1})))^2 \rightarrow S_k(\Gamma_1(N))$$

by

$$(f, g) \mapsto f + g[\alpha_d]_k.$$

The **subspace of oldforms** at level N is defined as a subspace of $S_k(\Gamma_1(N))$ by

$$S_k(\Gamma_1(N))^{old} = \sum_{p|N, p \text{ prime}} i_p(S_k(\Gamma_1(Nd^{-1})))^2$$

The **subspace of newforms** at level N is the orthogonal complement with respect to the Petersson inner product $S_k(\Gamma_1(N))^{new} = (S_k(\Gamma_1(N))^{old})^\perp$.

Both $S_k(\Gamma_1(N))^{new}$ and $S_k(\Gamma_1(N))^{old}$ are stable under T_n and $\langle n \rangle$ for all $n \in \mathbb{Z}^+$ (see 5.6.2 in [DS]).

A nonzero modular form $f \in M_k(\Gamma_1(N))$ which is an eigenform for the Hecke operators T_n and $\langle n \rangle$ for all $n \in \mathbb{Z}^+$ is called a **Hecke eigenform** or simply an **eigenform**. The eigenform $f(z) = \sum_{n=0}^{\infty} a_n(f)q^n$ (where $q = e^{2\pi iz}$) is **normalized** if $a_1(f) = 1$. A normalized eigenform in $S_k(\Gamma_1(N))^{new}$ is called a **newform**. Newforms form an orthogonal basis of $S_k(\Gamma_1(N))^{new}$ (see 5.8.2 of [DS]).

Let us show an example involving modular forms computed by **SAGE**:

```
sage: S = CuspForms(Gamma1(13), 2, prec = 15)
Cuspidal subspace of dimension 2 of Modular Forms space of dimension 13
for Congruence Subgroup Gamma1(13) of weight 2 over Rational Field
sage: S.basis()
[
q - 4 * q^3 - q^4 + 3 * q^5 + 6 * q^6 - 3 * q^8 + q^9 - 6 * q^10 - 2 * q^12 + 2 * q^13 + O(q^15),
q^2 - 2 * q^3 - q^4 + 2 * q^5 + 2 * q^6 - 2 * q^8 + q^9 - 3 * q^10 + 3 * q^13 + O(q^15)
]
sage: S.new_subspace().basis()
[
q - 4 * q^3 - q^4 + 3 * q^5 + 6 * q^6 - 3 * q^8 + q^9 - 6 * q^10 - 2 * q^12 + 2 * q^13 + O(q^15),
q^2 - 2 * q^3 - q^4 + 2 * q^5 + 2 * q^6 - 2 * q^8 + q^9 - 3 * q^10 + 3 * q^13 + O(q^15)
]
```

This example points to a more general fact: for N prime and $k \leq 11$ we have $S_k(\Gamma_1(N))^{new} = S_k(\Gamma_1(N))$.

For an introduction to **SAGE** in the context of modular forms see [Stein].

L-functions

Let us write $f \in M_k(\Gamma_1(N))$ as $f(z) = \sum_{n=0}^{\infty} a_n(f)q^n$ where $q = e^{2\pi iz}$. We can associate to f an **L-function** by

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

It converges absolutely in the strip $\operatorname{Re}(s) > k/2 + 1$ when f is a cusp form, and in the strip $\operatorname{Re}(s) > k$ when it is not a cusp form (see 5.9.1 of [DS]).

A condition that f is a normalized eigenform is equivalent to $L(s, f)$ having an Euler product expansion:

$$L(s, f) = \prod_{p \text{ prime}} (1 - a_p(f)p^{-s} + p^{k-1-2s})^{-1}.$$

Jacobians and abelian varieties

The **Jacobian** $Jac(X)$ of a compact Riemann surface X is equal to $\Omega_{hol}^1(X)^\wedge/H_1(X, \mathbb{Z})$, where $^\wedge$ denotes the dual space.

We view X as a sphere with g handles, where g is the genus of X . Let A_1, \dots, A_g be longitudinal loops around each handle-like arm-bands and let B_1, \dots, B_g be latitudinal loops around each handle-like equators. Then

$$\Omega_{hol}^1(X)^\wedge \cong \mathbb{R} \int_{A_1} \oplus \dots \oplus \mathbb{R} \int_{A_g} \oplus \mathbb{R} \int_{B_1} \oplus \dots \oplus \mathbb{R} \int_{B_g},$$

whereas $H_1(X, \mathbb{Z})$ is embedded into $\Omega_{hol}^1(X)^\wedge$ as

$$\mathbb{Z} \int_{A_1} \oplus \dots \oplus \mathbb{Z} \int_{A_g} \oplus \mathbb{Z} \int_{B_1} \oplus \dots \oplus \mathbb{Z} \int_{B_g}.$$

Let us denote $Jac(X_0(N)), Jac(X_1(N))$ by $J_0(N), J_1(N)$, respectively.

By using the isomorphism between $S_2(\Gamma)$ and $\Omega_{hol}^1(X(\Gamma))$ we can write:

$$Jac(X(\Gamma)) = S_2(\Gamma)^\wedge/H_1(X(\Gamma), \mathbb{Z}).$$

We have an action of $T_{\mathbb{Z}}$ on $S_2(\Gamma_1(N))$ and hence on $S_2(\Gamma_1(N))^\wedge$ by composition. This action descends to an action of $T_{\mathbb{Z}}$ on $J_1(N)$ by $[\phi] \mapsto [\phi \circ T]$ for $\phi \in S_2(\Gamma_1(N))^\wedge$ (see 6.3.2 in [DS]). As there is a surjection from $J_1(N)$ to $J_0(N)$ we also have an action of $T_{\mathbb{Z}}$ on $J_0(N)$ (a surjection comes from an inclusion $\Gamma_1(N) \subset \Gamma_0(N)$; this induces the map $S_2(\Gamma_1(N))^\wedge \rightarrow S_2(\Gamma_0(N))^\wedge$ which descends to a map on Jacobians).

Let $f(z) = \sum_{n=0}^{\infty} a_n(f)q^n$ be a normalized eigenform. Let us define a homomorphism $\lambda_f : T_{\mathbb{Z}} \rightarrow \mathbb{C}$ by $Tf = \lambda_f(T)f$. This homomorphism has as its image $\mathbb{Z}\{a_n(f) : n \in \mathbb{Z}^+\}$. Setting $I_f = \ker(\lambda_f) = \{T \in T_{\mathbb{Z}} : Tf = 0\}$ we have a \mathbb{Z} -module isomorphism $T_{\mathbb{Z}}/I_f \cong \mathbb{Z}\{a_n(f) : n \in \mathbb{Z}^+\}$.

Now to a newform $f \in S_2(\Gamma_1(N))$ we can associate an abelian variety (see 6.6 of [DS]). This can be done in the following way. Since $T_{\mathbb{Z}}$ acts on $J_1(N)$, the subgroup $I_f J_1(N)$ of $J_1(N)$ makes sense and we can set

$$A_f = J_1(N)/I_f J_1(N).$$

In the same way we let

$$A'_f = J_0(N)/I_f J_0(N)$$

for each newform $f \in S_2(\Gamma_0(N))$.

Galois representations

Having constructed an abelian variety A_f for each normalized eigenform f of weight 2, we can define its Tate module just like in the case of elliptic curves: $T_l(A_f) = \varprojlim A_f[l^n]$. This leads to a Galois representation $\rho_{A_f, l} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_{2d}(\mathbb{Q}_l)$, where d is the dimension of A_f . Nevertheless, we would like to have a representation which goes to GL_2 .

Let us tensor the Tate module with \mathbb{Q} to obtain $V_l(A_f) = T_l(A_f) \otimes \mathbb{Q}$. We set $O_f = \mathbb{Z}[\{a_n(f) : n \in \mathbb{Z}^+\}]$. The **number field** of f is denoted by $K_f = O_f \otimes \mathbb{Q}$. As $T_{\mathbb{Z}}/I_f \cong O_f$, observe that O_f acts on A_f . Each $a_p(f)$ acts on A_f as $T_p + I_f$. Thus, O_f acts also on the Tate module of A_f and hence $T_l(A_f)$ is an O_f -module, so $V_l(A_f)$ is a module over $O_f \otimes \mathbb{Q}_l = K_f \otimes_{\mathbb{Q}} \mathbb{Q}_l$.

It can be proved that $V_l(A_f)$ is a free module of rank 2 over $K_f \otimes_{\mathbb{Q}} \mathbb{Q}_l$ (see 9.5.3 of [DS]). Therefore $V_l(A_f) \cong (K_f \otimes_{\mathbb{Q}} \mathbb{Q}_l)^2$.

As $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts $K_f \otimes_{\mathbb{Q}} \mathbb{Q}_l$ -linearly on $V_l(A_f)$, we get after choosing a basis for $V_l(A_f)$ a homomorphism $\text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(K_f \otimes_{\mathbb{Q}} \mathbb{Q}_l)$. By a standard fact from the algebraic number theory (see II.8.3 of [Neu]) we can write $K_f \otimes_{\mathbb{Q}} \mathbb{Q}_l$ as a product of localisations of K_f over different places, i.e. $K_f \otimes_{\mathbb{Q}} \mathbb{Q}_l \cong \prod_{\lambda|l} K_{f, \lambda}$. Composing the above homomorphism with a projection we get a Galois representation:

$$\rho_{f, \lambda} : \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(K_{f, \lambda})$$

Remark: A Galois representation can be associated to a normalized eigenform of arbitrary weight. For weight one see [Del-Se], for weight greater than two see [Del].

Let G be a group and V a finite dimensional vector space. Let us recall that two representations $\rho_1, \rho_2 : G \rightarrow \text{GL}(V)$ are similar if there exists an element $m \in \text{GL}(V)$ such that $\rho_1(\sigma) = m^{-1} \rho_2(\sigma) m$ for all $\sigma \in G$. We write $\rho_1 \sim \rho_2$.

Modularity

After all the preliminaries, in this section we state the main result we have strived for: the Modularity Theorem in different forms. I use freely the notation introduced in the preceding sections. All of the following theorems can be shown to be equivalent (see [DS]).

Modularity Theorem (version X_C , 2.5.1 of [DS]) Let E be a complex elliptic curve with $j(E) \in \mathbb{Q}$. Then for some positive integer N there exists a surjective holomorphic function of compact Riemann surfaces: $X_0(N) \rightarrow E$.

Modularity Theorem (version J_C , 6.1.3 of [DS]) Let E be a complex elliptic curve with $j(E) \in \mathbb{Q}$. Then for some positive integer N there exists a surjective holomorphic homomorphism of complex tori: $J_0(N) \rightarrow E$.

Modularity Theorem (version a_p , 8.8.1 of [DS]) Let E be an elliptic curve over \mathbb{Q} with conductor N . Then for some newform $f \in S_2(\Gamma_0(N))$, $a_p(f) = a_p(E)$ for all primes p .

Modularity Theorem (strong version A_Q , 8.8.4 of [DS]) Let E be an elliptic curve over \mathbb{Q} with conductor N . Then for some newform $f \in S_2(\Gamma_0(N))$, the abelian variety A'_f is also an elliptic curve over \mathbb{Q} and there exists an isogeny $A'_f \rightarrow E$ defined over \mathbb{Q} .

Modularity Theorem (strong version R , 9.6.3 of [DS]) Let E be an elliptic curve over \mathbb{Q} with conductor N . Then for some newform $f \in S_2(\Gamma_0(N))$ with number field $K_f = \mathbb{Q}$, we have $p_{f,l} \sim p_{E,l}$ for all l .

Serre's conjecture

Let $f \in S_2(\Gamma_1(M))$ be a newform and let $\lambda \subset O_f$ be an ideal lying over l . Let us recall that by 9.3.5 of [DS] each representation $\rho : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow GL_d(L)$ is similar to a Galois representation $\rho' : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow GL_d(O_L)$ where L is a number field and O_L is its ring of integers. Therefore we can assume that $\rho_{f,\lambda}$ maps to $GL_2(O_{f,\lambda})$ and thus $\rho_{f,\lambda}$ has mod l reduction $\overline{\rho_{f,\lambda}} : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow GL_2(O_{f,\lambda}/\lambda O_{f,\lambda})$.

An irreducible representation $\rho : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow GL_2(\overline{\mathbb{F}}_l)$ is **modular of level M** if there exists a newform $f \in S_2(\Gamma_1(M))$ and a maximal ideal $\lambda \subset O_f$ lying over l such that $\overline{\rho_{f,\lambda}} \sim \rho$. We can now formulate (though we do not write explicitly $M(\rho)$):

Serre's conjecture: $\rho : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow GL_2(\overline{\mathbb{F}}_l)$ be irreducible and odd. Then ρ is modular of level $M(\rho)$.

Serre's conjecture was finally proved by Khare (with a help of Wintenberger) in 2006. See [KW1],[KW2] or [K].

Example

Let p be an odd prime. Consider an elliptic curve $E_p : y^2 = x^3 + px$. This is an elliptic curve with j -invariant 1728 (all such curves are isomorphic over $\overline{\mathbb{Q}}$). It has additive reductions at 2 and p and good reductions elsewhere (see Proposition 5.1 of Chapter VII in [Silv1]). Let q be a prime different from 2 and p . Interpreting $(x^3 + px)^{(q-1)/2}$ as $-1, 0, 1$ according to its value in \mathbb{F}_q , we see that:

$$|E_p(\mathbb{F}_q)| = 1 + q + \sum_{x \in \mathbb{F}_q} (x^3 + px)^{(q-1)/2}.$$

Now we have the following equalities modulo q

$$\sum_{x \in \mathbb{F}_q} (x^3 + px)^{(q-1)/2} = \sum_{i=0}^{q-2} (\lambda^{3i} + p\lambda^i)^{(q-1)/2} = \sum_{k=0}^{(q-1)/2} \binom{(q-1)/2}{k} p^{(q-1)/2-k} \sum_{i=0}^{q-2} \lambda^{i(2k+(q-1)/2)},$$

where λ is a generator of \mathbb{F}_q^* . It can be easily seen that $\sum_{i=0}^{q-2} \lambda^{i(2k+(q-1)/2)}$ is non-zero (and then it is equal to $q-1$) modulo q if and only if $2k + (q-1)/2 = q-1$, i.e. $k = (q-1)/4$. Hence we get

$$\sum_{x \in \mathbb{F}_q} (x^3 + px)^{(q-1)/2} \equiv \begin{cases} -\binom{(q-1)/2}{(q-1)/4} p^{(q-1)/4}, & \text{when } q \equiv 1 \pmod{4}, \\ 0, & \text{otherwise.} \end{cases}$$

Recall that $a_q = q + 1 - |E_p(\mathbb{F}_q)|$ hence we have computed the L-function associated with E_p , namely:

$$\begin{aligned} L_{E_p}(s) &= \prod_{q \neq 2, p} (1 - a_q q^{-s} + q^{1-2s})^{-1} \\ &= \prod_{\substack{q \equiv 3 \pmod{4} \\ q \neq p}} (1 + q^{1-2s})^{-1} \prod_{\substack{q \equiv 1 \pmod{4} \\ q \neq p}} \left(1 - \left(\binom{(q-1)/2}{(q-1)/4} p^{(q-1)/4} \text{ mod } q \right) q^{-s} + q^{1-2s} \right)^{-1}. \end{aligned}$$

In the above formula $\binom{(q-1)/2}{(q-1)/4} p^{(q-1)/4} \text{ mod } q$ denotes the integer congruent to $\binom{(q-1)/2}{(q-1)/4} p^{(q-1)/4}$ modulo q for which Hasse-Weil inequality holds: $|a_q| \leq 2\sqrt{q}$ (there is only one such integer).

We can calculate the conductor $f(E_p/\mathbb{Q})$ of E_p using Tate's algorithm (see IV.9 in [Silv2]) obtaining $f(E_p/\mathbb{Q}) = 2^{5+a} p^2$, where

$$a = \begin{cases} 1 & \text{if } p \equiv 1 \pmod{4}, \\ 0 & \text{if } p \equiv 3 \pmod{4}. \end{cases}$$

Now we can formulate the Modularity Theorem more explicitly. First of all, there exists a surjective map $X_0(2^{5+a} p^2) \rightarrow E_p$. Moreover, there exists a newform $f \in S_2(\Gamma_0(2^{5+a} p^2))$ such that $a_q(f) = a_q(E_p)$ for all primes q . This determines f completely though there is not much chance to compute f in more explicit terms as $S_2(\Gamma_0(2^{5+a} p^2))$ has large dimension (for example, for $p = 5$, the conductor is equal to 1600 and the dimension of $S_2(\Gamma_0(1600))$ is 205).

Let us also show an example of how $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ acts on torsion points, giving rise to a Galois representation. Using the group law algorithm (see III.2.3 of [Silv1]), we calculate for $P = (x, y)$:

$$x([2]P) = \frac{(x^2 - p)^2}{4x^3 + 4px}.$$

Hence E_p has only the following 2-torsion points:

$$E_p[2] = \{P_1 = (p^{1/2}, p^{3/4}), P_2 = (p^{1/2}, -p^{3/4}), P_3 = (-p^{1/2}, ip^{3/4}), P_4 = (-p^{1/2}, -ip^{3/4})\}.$$

Since $P_1 = -P_2$ and $P_3 = -P_4$ we can pick P_1 and P_3 as a basis for $E_p[2]$. Because $E_p[2] \subset Gal(\mathbb{Q}(p^{1/4}, i)/\mathbb{Q})$, the representation $\rho : Gal(\overline{\mathbb{Q}}/\mathbb{Q}) \rightarrow Aut(E_p[2])$ arising from an action of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ on 2-torsion points factors through $Gal(\mathbb{Q}(p^{1/4}, i)/\mathbb{Q})$. It is easy to see that σ, τ such that $\sigma(i) = -i$, $\sigma(p^{1/4}) = p^{1/4}$ and $\tau(i) = i$, $\tau(p^{1/4}) = ip^{1/4}$ generate $Gal(\mathbb{Q}(p^{1/4}, i)/\mathbb{Q})$. Now observe that $\sigma P_1 = P_1$, $\sigma P_3 = P_4 = -P_3$ and $\tau P_1 = P_3$, $\tau P_3 = P_1$ and hence our Galois representation can be written as

$$\rho(\sigma) = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}, \quad \rho(\tau) = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$$

with respect to the basis P_1, P_3 of $Aut(E_p[2])$.

As the final remark, note that ρ is a part of $\rho_{E_p, 2}$ - the representation arising from an action of $Gal(\overline{\mathbb{Q}}/\mathbb{Q})$ on the Tate module $T_2(E_p) = \varprojlim E_p[2^n]$.

Bibliografia

- [BCDT] Ch. Breuil, B. Conrad, F. Diamond, R. Taylor, On the modularity of elliptic curves over \mathbb{Q} : wild 3-adic exercises, *J. Amer. Math. Soc.* **14** (2001), 843–939.
- [Cais] B. Cais, Serre’s conjectures, in Cornell, Stevens, Silverman, *Modular Forms and Fermat’s Last Theorem*, Springer-Verlag, 1997.
- [DS] F. Diamond, J. Shurman, *A first course in the modular forms*, Springer Science+Business Media, Inc. New York, 2005.
- [Del] P. Deligne, Formes modulaires et représentations l -adiques, *Séminaire Bourbaki* **11** (1968-1969), Exp. No. 355.
- [Del-Se] P. Deligne, J.-P. Serre, Formes modulaires de poids 1, *Ann. Sci. École Norm. Sup.* **7** (1974), 507–530 (1974).
- [Har] R. Hartshorne, Algebraic geometry, *Graduate Texts in Mathematics* **52**, Springer-Verlag, New York, 1977.
- [K] Ch. Khare, Serres modularity conjecture: the level one case, *Duke Math. J.* **134** (2006), 557–589.
- [KW1] Ch. Khare, J.-P. Wintenberger, Serre’s modularity conjecture (I), preprint, available at <http://www.math.utah.edu/~shekhar/papers.html>.
- [KW2] Ch. Khare, J.-P. Wintenberger, Serre’s modularity conjecture (II), preprint. available at <http://www.math.utah.edu/~shekhar/papers.html>.
- [Neu] J. Neukirch, Algebraic number theory, *Grundlehren der Mathematischen Wissenschaften* **322**, Springer Verlag, 1999.
- [Silv1] J. H. Silverman, The arithmetic of elliptic curves, *Graduate Texts in Mathematics* **106**, Springer-Verlag, 1986.
- [Silv2] J. H. Silverman, Advanced topics in the arithmetic of elliptic curves, *Graduate Texts in Mathematics* **151**, Springer-Verlag, 1995.
- [Stein] W. A. Stein, Modular forms: a computational approach, preprint, available at <http://modular.math.washington.edu/books/modform/>.
- [TW] R. Taylor, A. Wiles, Ring-theoretic properties of certain Hecke algebras, *Ann. of Math.* **141** (1995), 553–572.
- [W] A. Wiles, Modular elliptic curves and Fermat’s last theorem, *Ann. of Math.* **141** (1995), 443–551.