Modular forms modulo p

Master's thesis defence

Francesc Gispert

under the supervision of

Adrian Iovita and Matteo Longo

16th July 2018

Elliptic curves

Definition

- An elliptic curve over a scheme S is a proper smooth morphism of schemes $\pi\colon E \to S$ whose geometric fibres are connected curves of genus 1 together with a section $e\colon S \to E$.

$$\begin{array}{c} E \\ \pi \Big\downarrow \; \Big\uparrow e \\ S \end{array}$$

- E admits a unique structure of abelian group scheme over S for which e is the identity section.
- Define the invertible $\mathscr{O}_S$–module $\underline{\omega}_{E/S} = \pi_*(\Omega^1_{E/S})$.
- $\underline{\omega}_{E/S}$ is the Serre–Grothendieck dual of $\mathrm{R}^1\pi_*(\mathscr{O}_E)$.
  - We identify $\mathrm{R}^1\pi_*(\mathscr{O}_E)$ with $\underline{\omega}_{E/S}^{\otimes -1}$.

Elliptic curves

Level $\Gamma(N)$–structures

- Let $N \in \mathbb{N}$.
- A level $\Gamma(N)$–structure on E/S is an isomorphism

$$\alpha_N\colon E[N] \xrightarrow{\cong} (\mathbb{Z}/N\mathbb{Z})^2_S$$

  of group schemes.
- N has to be invertible in $\mathrm{H}^0(S, \mathscr{O}_S)$.

Elliptic curves

Test objects of level $\Gamma(N)$

- From now on, fix $N \in \mathbb{N}$.
- Let K be a ring with $N \in K^\times$.
- We consider pairs $(E/S, \alpha_N)$, where
  - S is a K–scheme,
  - E is an elliptic curve over S and
  - α_N is a level $\Gamma(N)$–structure on E/S.

Modular forms

Definition

- Let $k \in \mathbb{Z}$.
- A modular form for $\Gamma(N)$ of weight k defined over K is a *rule* f which assigns to each pair $(E/S, \alpha_N)$ an element $f(E/S, \alpha_N) \in \mathrm{H}^0(S, \underline{\omega}_{E/S}^{\otimes k})$ satisfying the following conditions:
  1. $f(E/S, \alpha_N)$ depends only on the S–isomorphism class of $(E/S, \alpha_N)$, and
  2. for every $g\colon S' \to S$, $f(g^*(E/S, \alpha_N)) = g^*(f(E/S, \alpha_N))$.

- If $S = \mathrm{Spec}(R)$ and there is a basis ω of $\underline{\omega}_{E/S}$, then we can express

$$f(E/S, \alpha_N) = f(E/S, \omega, \alpha_N) \cdot \omega^{\otimes k}$$

  for some $f(E/S, \omega, \alpha_N) \in R$.
- This leads to an alternative definition of modular forms as *rules* which assign values to triples $(E/R, \omega, \alpha_N)$.

Modular forms

q–expansions

- Suppose that K contains a primitive N–th root of unity.
- Consider the Tate curve $\mathrm{Tate}(q)$ over $K((q^{1/N}))$ with its canonical differential ω_{can}.

- The q–expansions of a modular form f for $\Gamma(N)$ defined over K are the series

$$\widehat{f}_{\alpha_N}(q) = f(\mathrm{Tate}(q)/K((q^{1/N})), \omega_{\mathrm{can}}, \alpha_N) \in K((q^{1/N}))$$

for the level $\Gamma(N)$–structures α_N on $\mathrm{Tate}(q)/K((q^{1/N}))$.

- Write $F(K;\Gamma(N),k)$ for the K–module of modular forms for $\Gamma(N)$ of weight k defined over K.
- Set

$$F(K;\Gamma(N)) = \bigoplus_{k\in\mathbb{Z}} F(K;\Gamma(N),k)\,.$$

Theorem

If $N \geq 3$, there exist

1. *a smooth affine curve $Y = Y(N)$ over K, called the modular curve (without cusps),*
2. *a universal elliptic curve $\pi\colon \mathbb{E} \to Y$ and*
3. *a universal level $\Gamma(N)$–structure α_{univ} on $\mathbb{E}/Y$*

with the following universal property: for each pair $(E/S, \alpha_N)$, there exists a unique K–morphism $g\colon S \to Y$ such that $E \cong \mathbb{E} \times_Y S$ and $\alpha_N = g^*(\alpha_{\mathrm{univ}})$.

Modular forms

Modular curves

- In the previous situation, we have a cartesian diagram

$$\begin{array}{ccc}(E,\alpha_N) & \longrightarrow & (\mathbb{E},\alpha_{\text{univ}}) \\ \downarrow & \ulcorner & \downarrow \pi \\ S & \xrightarrow{\;g\;} & Y\end{array}$$

(i.e., $(E/S,\alpha_N) \cong g^*(\mathbb{E}/Y,\alpha_{\text{univ}})$).

Modular forms

Alternative definition

- Write $\underline{\omega} = \underline{\omega}_{\mathbb{E}/Y}$.
- A modular form $f \in F(K; \Gamma(N), k)$ is uniquely determined by its value
$$f(\mathbb{E}/Y, \alpha_{\mathrm{univ}}) \in \mathrm{H}^0(Y, \underline{\omega}^{\otimes k}) .$$
- Hence, we identify $F(K; \Gamma(N), k) = \mathrm{H}^0(Y, \underline{\omega}^{\otimes k})$.

Modular forms modulo p

Notation

- Throughout the rest of this presentation:
  - Let K be an algebraically closed field of characteristic $p > 0$.
  - Suppose that $N \geq 3$ and $p \nmid N$.

Modular forms modulo p

De Rham cohomology

- There is a short exact sequence

$$\begin{array}{ccccccccc} 0 & \longrightarrow & R^0\pi_*(\Omega^1_{\mathbb{E}/Y}) & \longrightarrow & H^1_{dR}(\mathbb{E}/Y) & \longrightarrow & R^1\pi_*(\mathscr{O}_{\mathbb{E}}) & \longrightarrow & 0 \\ \| & & \| & & \| & & \|\wr & & \| \\ 0 & \longrightarrow & \underline{\omega} & \longrightarrow & H^1_{dR}(\mathbb{E}/Y) & \longrightarrow & \underline{\omega}^{\otimes -1} & \longrightarrow & 0 \end{array}$$

given by the Hodge filtration for $\mathbb{E}/Y$.

- Locally on Y, $\mathrm{H}^1_{\mathrm{dR}}(\mathbb{E}/Y)$ admits a basis (ω, η) such that
  - ω is a local basis of $\underline{\omega}$ and
  - the projection $\widetilde{\eta}$ of η on $\underline{\omega}^{\otimes -1}$ is the dual of ω.

Modular forms modulo p

Frobenius

- In characteristic p, the p–th power map gives the absolute Frobenius endomorphism

$$\mathrm{Frob}_{\mathbb{E}} : \mathbb{E} \to \mathbb{E}$$

(it is not a Y–morphism).

Modular forms modulo p

The Hasse invariant

- $\mathrm{Frob}_{\mathbb{E}}$ induces $\mathrm{Frob}_{\mathbb{E}}^{*} \colon \mathrm{R}^1\pi_*(\mathscr{O}_{\mathbb{E}}) \to \mathrm{R}^1\pi_*(\mathscr{O}_{\mathbb{E}})$.
- Thus, locally on Y,

$$\mathrm{Frob}_{\mathbb{E}}^{*}(\widetilde{\eta}) = A(\mathbb{E}/Y, \omega)\widetilde{\eta}$$

for some section $A(\mathbb{E}/Y, \omega)$ of $\mathscr{O}_Y$.

Modular forms modulo p

The Hasse invariant

- $A(\mathbb{E}/Y, \omega)$ defines a modular form for $\Gamma(1)$ of weight $p-1$.
- $A \in F(K; \Gamma(N), p-1)$ is called the Hasse invariant.

Lemma

The q–expansions of A are all equal to 1.

Modular forms modulo p

The structure theorem

Theorem

The kernel of the map

$$F(K;\Gamma(N)) \to \prod_{\alpha_N} K((q^{1/N}))$$

mapping modular forms to their q–expansions is the ideal generated by $A-1$.

Theorem

There is a derivation

$$A\theta\colon F(K;\Gamma(N),\bullet) \to F(K;\Gamma(N),\bullet+p+1)$$

whose effect on q–expansions is $q\dfrac{d}{dq}$.

Modular forms modulo p

The locus where A is invertible

- Let $\mathscr{F} = \mathrm{Im}\big(\mathrm{Frob}_{\mathbb{E}}^{*} \colon \mathrm{H}^1_{\mathrm{dR}}(\mathbb{E}/Y) \to \mathrm{H}^1_{\mathrm{dR}}(\mathbb{E}/Y)\big)$.
- Let Y^{H} be the open subset of Y where A is invertible.

Modular forms modulo p

The locus where A is invertible

Lemma

Y^{H} is the largest open subset of Y over which the map

$$\underline{\omega} \oplus \mathscr{F} \to \mathrm{H}^1_{\mathrm{dR}}(\mathbb{E}/Y)$$

induced by the inclusions is an isomorphism.

- Let $k \in \mathbb{N}$.
- Over Y^{H}, we have a decomposition

$$\mathrm{Sym}^k \mathrm{H}^1_{\mathrm{dR}}(\mathbb{E}/Y)\big|_{Y^{\mathrm{H}}} \cong \left[\underline{\omega}^{\otimes k} \oplus (\underline{\omega}^{\otimes k-1} \otimes_{\mathscr{O}_Y} \mathscr{F}) \oplus \cdots \oplus \mathscr{F}^{\otimes k}\right]\big|_{Y^{\mathrm{H}}}.$$

- We define $\theta\colon \mathrm{H}^0(Y^{\mathrm{H}}, \underline{\omega}^{\otimes k}) \to \mathrm{H}^0(Y^{\mathrm{H}}, \underline{\omega}^{\otimes k+2})$ to be the following composition:

Modular forms modulo p

The operator θ

$$
\begin{array}{cccl}
\underline{\omega}^{\otimes k}\big|_{Y^{\mathrm{H}}} & \hookrightarrow & & \mathrm{Sym}^k\, \mathrm{H}^1_{\mathrm{dR}}(\mathbb{E}/Y)\big|_{Y^{\mathrm{H}}} \cong \underline{\omega}^{\otimes k}\big|_{Y^{\mathrm{H}}} \oplus \cdots \\
 & & & \downarrow \nabla \\
 & & & \mathrm{Sym}^k\, \mathrm{H}^1_{\mathrm{dR}}(\mathbb{E}/Y)\big|_{Y^{\mathrm{H}}} \otimes \Omega^1_{Y^{\mathrm{H}}/K} \\
 & & & \wr\!\!\parallel \downarrow \mathrm{KS}^{-1} \\
 & & & \mathrm{Sym}^k\, \mathrm{H}^1_{\mathrm{dR}}(\mathbb{E}/Y)\big|_{Y^{\mathrm{H}}} \otimes \underline{\omega}^{\otimes 2}\big|_{Y^{\mathrm{H}}} \cong \underline{\omega}^{\otimes k+2}\big|_{Y^{\mathrm{H}}} \oplus \cdots \\
 & & & \qquad\qquad\qquad\qquad\qquad\qquad \twoheaddownarrow \\
 & \overset{\theta}{\dashrightarrow} & & \qquad\qquad\qquad\qquad\qquad\qquad \underline{\omega}^{\otimes k+2}\big|_{Y^{\mathrm{H}}}
\end{array}
$$

Modular forms modulo p

The operator $A\theta$

Lemma

There exists a unique map

$$A\theta \colon F(K;\Gamma(N),k) \to F(K;\Gamma(N),k+p+1)$$

making the diagram

$$\begin{array}{ccccc} \mathrm{H}^0(Y^{\mathrm{H}},\underline{\omega}^{\otimes k}) & \xrightarrow{\theta} & \mathrm{H}^0(Y^{\mathrm{H}},\underline{\omega}^{\otimes k+2}) & \xrightarrow{\cdot A} & \mathrm{H}^0(Y^{\mathrm{H}},\underline{\omega}^{\otimes k+p+1}) \\ \uparrow & & & & \uparrow \\ \mathrm{H}^0(Y,\underline{\omega}^{\otimes k}) & & \xrightarrow{A\theta} & & \mathrm{H}^0(Y,\underline{\omega}^{\otimes k+p+1}) \end{array}$$

commute.

Summary

- Let K be an algebraically closed field of characteristic $p > 0$ and let $N \geq 3$ such that $p \nmid N$.
- The K–algebra $F(K;\Gamma(N))$ can be described in terms of q–expansions (i.e., power series in $q^{1/N}$) and the Hasse invariant A.
- Namely, A is *essentially* the only modular form (apart from the constant 1) whose q–expansions are equal to 1.
- Moreover, there is a derivation

$$A\theta\colon F(K;\Gamma(N),\bullet) \to F(K;\Gamma(N),\bullet + p + 1)$$

with a very simple expression on q–expansions and which allows us to find some relations in $F(K;\Gamma(N))$ using powers of A.