The Eisenstein quotient

Reading Group Mazur's Theorem

fall 2020

Where we left

Fix $N \geq 11$ prime, $N \neq 13$ (so $g = g(X_0(N)) > 0$).
Goal: construct a quotient A of $J_0(N)$ so that

- $X_0(N) \to A$ seperates the cusps
- $A(\mathbb{Q})$ has rank 0

Where we left

Fix $N \geq 11$ prime, $N \neq 13$ (so $g = g(X_0(N)) > 0$).
Goal: construct a quotient A of $J_0(N)$ so that

- $X_0(N) \to A$ seperates the cusps
- $A(\mathbb{Q})$ has rank 0

As A has good reduction outside N, we have seen that this implies there exist no rational elliptic curves with N-torsion, i.e. $Y_1(N)(\mathbb{Q}) = \emptyset$.

Intermezzo on reduction of $X_0(N)$

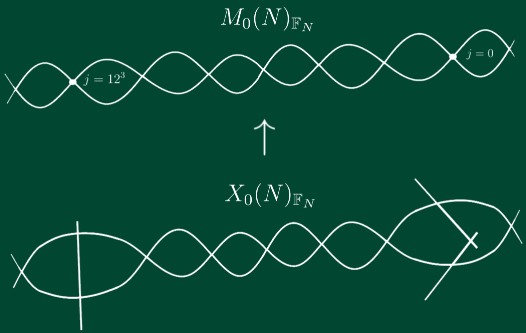
The coarse moduli space $M_0(N)/\mathbb{Z}$ classifying generalised elliptic curves with level $\Gamma_0(N)$-structure is fine over $\mathbb{Z}[1/N]$.

Intermezzo on reduction of $X_0(N)$

The coarse moduli space $M_0(N)/\mathbb{Z}$ classifying generalised elliptic curves with level $\Gamma_0(N)$-structure is fine over $\mathbb{Z}[1/N]$. Obtain $X_0(N)$ by desingularising special fiber $M_0(N)$ at N:

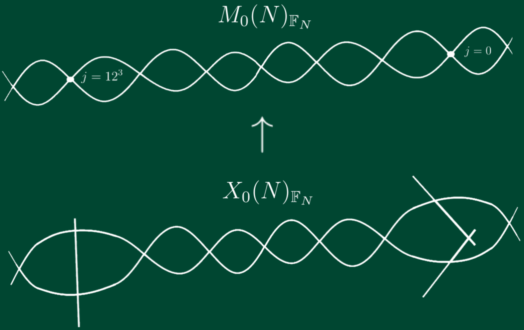
Intermezzo on reduction of $X_0(N)$

The coarse moduli space $M_0(N)/\mathbb{Z}$ classifying generalised elliptic curves with level $\Gamma_0(N)$-structure is fine over $\mathbb{Z}[1/N]$. Obtain $X_0(N)$ by desingularising special fiber $M_0(N)$ at N:



Intermezzo on reduction of $X_0(N)$

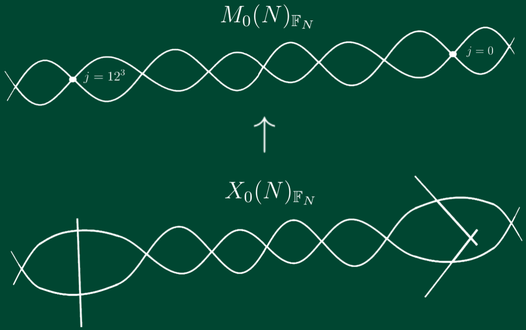
The coarse moduli space $M_0(N)/\mathbb{Z}$ classifying generalised elliptic curves with level $\Gamma_0(N)$-structure is fine over $\mathbb{Z}[1/N]$. Obtain $X_0(N)$ by desingularising special fiber $M_0(N)$ at N:



Néron model of $J_0(N)/\mathbb{Q}$ is smooth outside N and totally toric at N.

Intermezzo on reduction of $X_0(N)$

The coarse moduli space $M_0(N)/\mathbb{Z}$ classifying generalised elliptic curves with level $\Gamma_0(N)$-structure is fine over $\mathbb{Z}[1/N]$. Obtain $X_0(N)$ by desingularising special fiber $M_0(N)$ at N:



Néron model of $J_0(N)/\mathbb{Q}$ is smooth outside N and totally toric at N. Any quotient A inherits these properties.

Overview

Reminders on $J_0(N)$ and the Hecke algebra

Construction of the Eisenstein Quotient

Main argument

Computation of α (the number of $\mathbb{Z}/p\mathbb{Z}$'s)

Computation of δ (the defect at N)

Recall:

- $S_2(\Gamma_0(N)) \cong H^0(X_0(N)_{\mathbb{C}}, \Omega^1)$

- Hodge decomposition

$$H^1(X_0(N)_{\mathbb{C}}, \mathbb{Z}) \otimes \mathbb{C} = S_2(\Gamma_0(N)) \oplus \overline{S_2(\Gamma_0(N))}$$

Recall:

- $S_2(\Gamma_0(N)) \cong H^0(X_0(N)_{\mathbb{C}}, \Omega^1)$
- Hodge decomposition

$$H^1(X_0(N)_{\mathbb{C}}, \mathbb{Z}) \otimes \mathbb{C} = S_2(\Gamma_0(N)) \oplus \overline{S_2(\Gamma_0(N))}$$

- Hecke correspondences on $X_0(N)$ form commutative ring $\mathbb{T}$, acting faithfully on $H^1(X_0(N)_{\mathbb{C}}, \mathbb{Z})$, hence finite free $\mathbb{Z}$-module

Recall:

- $S_2(\Gamma_0(N)) \cong H^0(X_0(N)_{\mathbb{C}}, \Omega^1)$ compatible with Hecke action
- Hodge decomposition

$$H^1(X_0(N)_{\mathbb{C}}, \mathbb{Z}) \otimes \mathbb{C} = S_2(\Gamma_0(N)) \oplus \overline{S_2(\Gamma_0(N))}$$

  compatible with Hecke action
- Hecke correspondences on $X_0(N)$ form commutative ring $\mathbb{T}$, acting faithfully on $H^1(X_0(N)_{\mathbb{C}}, \mathbb{Z})$, hence finite free $\mathbb{Z}$-module

Recall:

- $S_2(\Gamma_0(N)) \cong H^0(X_0(N)_{\mathbb{C}}, \Omega^1)$ compatible with Hecke action
- Hodge decomposition

$$H^1(X_0(N)_{\mathbb{C}}, \mathbb{Z}) \otimes \mathbb{C} = S_2(\Gamma_0(N)) \oplus \overline{S_2(\Gamma_0(N))}$$

  compatible with Hecke action
- Hecke correspondences on $X_0(N)$ form commutative ring $\mathbb{T}$, acting faithfully on $H^1(X_0(N)_{\mathbb{C}}, \mathbb{Z})$, hence finite free $\mathbb{Z}$-module
- $S_2(\Gamma_0(N))$ has a basis of normalised eigenforms; multiplicity one implies it is a free $\mathbb{T}_{\mathbb{C}}$-module of rank 1

Recall:

- $S_2(\Gamma_0(N)) \cong H^0(X_0(N)_{\mathbb{C}}, \Omega^1)$ compatible with Hecke action
- Hodge decomposition

$$H^1(X_0(N)_{\mathbb{C}}, \mathbb{Z}) \otimes \mathbb{C} = S_2(\Gamma_0(N)) \oplus \overline{S_2(\Gamma_0(N))}$$

  compatible with Hecke action
- Hecke correspondences on $X_0(N)$ form commutative ring $\mathbb{T}$, acting faithfully on $H^1(X_0(N)_{\mathbb{C}}, \mathbb{Z})$, hence finite free $\mathbb{Z}$-module
- $S_2(\Gamma_0(N))$ has a basis of normalised eigenforms; multiplicity one implies it is a free $\mathbb{T}_{\mathbb{C}}$-module of rank 1 and therefore $H^1(X_0(N), \mathbb{Q})$ free $\mathbb{T}_{\mathbb{Q}}$-module rank 2.

Recall:

- $S_2(\Gamma_0(N)) \cong H^0(X_0(N)_{\mathbb{C}}, \Omega^1)$ compatible with Hecke action
- Hodge decomposition

$$H^1(X_0(N)_{\mathbb{C}}, \mathbb{Z}) \otimes \mathbb{C} = S_2(\Gamma_0(N)) \oplus \overline{S_2(\Gamma_0(N))}$$

  compatible with Hecke action
- Hecke correspondences on $X_0(N)$ form commutative ring $\mathbb{T}$, acting faithfully on $H^1(X_0(N)_{\mathbb{C}}, \mathbb{Z})$, hence finite free $\mathbb{Z}$-module
- $S_2(\Gamma_0(N))$ has a basis of normalised eigenforms; multiplicity one implies it is a free $\mathbb{T}_{\mathbb{C}}$-module of rank 1 and therefore $H^1(X_0(N), \mathbb{Q})$ free $\mathbb{T}_{\mathbb{Q}}$-module rank 2.
- Dualizing and tensoring with $\mathbb{Q}_l$ where $(l \neq N)$, we see $V_l(J_0(N))$ is a rank 2 $\mathbb{T}_{\mathbb{Q}_l}$-module

have bijections:
$\{$normalised eigenforms$\} \leftrightarrow \{$homomorphisms $\mathbb{T} \to \mathbb{C}\} \leftrightarrow$
$\{$minimal primes of $\mathbb{T}\}$

have bijections:
$\{$normalised eigenforms$\} \leftrightarrow \{$homomorphisms $\mathbb{T} \to \mathbb{C}\} \leftrightarrow$
$\{$minimal primes of $\mathbb{T}\}$

Notation.

for $f \in S_2(\Gamma_0(N))$ normalised eigenform, denote $\mathfrak{p}_f$ for kernel of eigenvalue homomorphism $\mathbb{T} \to \mathbb{C}$, generated by $T_l - a_l(f)$ for $l \neq N$.

have bijections:
$\{$normalised eigenforms$\} \leftrightarrow \{$homomorphisms $\mathbb{T} \to \mathbb{C}\} \leftrightarrow$
$\{$minimal primes of $\mathbb{T}\}$

Notation.

for $f \in S_2(\Gamma_0(N))$ normalised eigenform, denote $\mathfrak{p}_f$ for kernel of eigenvalue homomorphism $\mathbb{T} \to \mathbb{C}$, generated by $T_l - a_l(f)$ for $l \neq N$.
Denote the image $\mathcal{O}_f$, it is an order in the (totally real) number field $K_f := \mathcal{O}_f \otimes \mathbb{Q}$.

have bijections:
$\{$normalised eigenforms$\} \leftrightarrow \{$homomorphisms $\mathbb{T} \to \mathbb{C}\} \leftrightarrow$ $\{$minimal primes of $\mathbb{T}\}$

Notation.

for $f \in S_2(\Gamma_0(N))$ normalised eigenform, denote $\mathfrak{p}_f$ for kernel of eigenvalue homomorphism $\mathbb{T} \to \mathbb{C}$, generated by $T_l - a_l(f)$ for $l \neq N$.
Denote the image $\mathcal{O}_f$, it is an order in the (totally real) number field $K_f := \mathcal{O}_f \otimes \mathbb{Q}$.

The abelian variety $A_f := J_0(N)/\mathfrak{p}_f J_0(N)$ has dimension $[K_f : \mathbb{Q}]$.
It is in fact simple (we won't need this).

Proposition.

$J_0(N)$ isogenous to $\prod_f A_f$ where f runs over the galois orbits of normalised eigenforms

Proposition.

$J_0(N)$ isogenous to $\prod_f A_f$ where f runs over the galois orbits of normalised eigenforms

Proof sketch.

Denote $e_f \in \mathbb{T}_{\mathbb{Q}} = \prod_f K_f$ for the idempotent of K_f, then for some $n > 0$, each ne_f lies in $\mathbb{T}$, so $n = \sum_f ne_f$. One checks $ne_f J_0(N) = A_f$, and so we get an isogeny $\prod_f A_f \to J_0(N)$ ■

Proposition.

$J_0(N)$ isogenous to $\prod_f A_f$ where f runs over the galois orbits of normalised eigenforms

Proof sketch.

Denote $e_f \in \mathbb{T}_{\mathbb{Q}} = \prod_f K_f$ for the idempotent of K_f, then for some $n > 0$, each ne_f lies in $\mathbb{T}$, so $n = \sum_f ne_f$. One checks $ne_f J_0(N) = A_f$, and so we get an isogeny $\prod_f A_f \to J_0(N)$ ■

Corollary.

$V_l J_0(N)$ decomposes as a product

$$V_l J_0(N) = \prod_f \prod_{\lambda \text{ in } K_f \text{ lying over } l} V_{f,\lambda},$$

where $V_{f,\lambda}$ are 2-dimensional λ-adic representations

Overview

Reminders on $J_0(N)$ and the Hecke algebra

Construction of the Eisenstein Quotient

Main argument

Computation of α (the number of $\mathbb{Z}/p\mathbb{Z}$'s)

Computation of δ (the defect at N)

Fix a prime p dividing the order of $[0] - [\infty] \in J_0(N)$
(last time we saw $[0] - [\infty]$ a nontrivial torsion element)

Fix a prime p dividing the order of $[0] - [\infty] \in J_0(N)$ (last time we saw $[0] - [\infty]$ a nontrivial torsion element)

Definition.

We define two ideals in $\mathbb{T}$

- The *p-Eisenstein prime* $\mathfrak{a}$ is generated by p and $T_l - (l+1)$ for $l \neq N$.

Fix a prime p dividing the order of $[0] - [\infty] \in J_0(N)$ (last time we saw $[0] - [\infty]$ a nontrivial torsion element)

Definition.

We define two ideals in $\mathbb{T}$

- The *p-Eisenstein prime* $\mathfrak{a}$ is generated by p and $T_l - (l+1)$ for $l \neq N$.
- The ideal I is the intersection of minimal primes in $\mathfrak{a}$:

$$I = \bigcap_{\mathfrak{p}_f \subset \mathfrak{a}} \mathfrak{p}_f = \bigcap_{n \geq 1} \mathfrak{a}^n.$$

The (p-)*Eisenstein quotient* is the abelian variety $A = J_0 N / I J_0(N)$

why $T_l - (l + 1)$?

why $T_l - (l+1)$?

Recall the Eichler-Shimura relation: if $\mathcal{A}/\mathbb{Z}$ is the Néron model of A, then for $l \neq N, p$, the Frobenius Frob_l satisfies

$$X^2 - T_l X + l \quad \text{in} \quad \mathrm{End}(\mathcal{A}_{\mathbb{F}_l})$$

why $T_l - (l+1)$?

Recall the Eichler-Shimura relation: if $\mathcal{A}/\mathbb{Z}$ is the Néron model of A, then for $l \neq N, p$, the Frobenius Frob_l satisfies

$$X^2 - T_l X + l \quad \text{in} \quad \mathrm{End}(\mathcal{A}_{\mathbb{F}_l})$$

If T_l acts like $l+1$, then this polynomial splits as

$$(X-l)(X-1).$$

why $T_l - (l+1)$?

Recall the Eichler-Shimura relation: if $\mathcal{A}/\mathbb{Z}$ is the Néron model of A, then for $l \neq N, p$, the Frobenius Frob_l satisfies

$$X^2 - T_l X + l \quad \text{in} \quad \mathrm{End}(\mathcal{A}_{\mathbb{F}_l})$$

If T_l acts like $l+1$, then this polynomial splits as

$$(X-l)(X-1).$$

This is similar to the representation $(\mathbb{Z}/p\mathbb{Z}) \oplus \mu_p$

why $T_l - (l+1)$?

Recall the Eichler-Shimura relation: if $\mathcal{A}/\mathbb{Z}$ is the Néron model of A, then for $l \neq N, p$, the Frobenius Frob_l satisfies

$$X^2 - T_l X + l \quad \text{in} \quad \mathrm{End}(\mathcal{A}_{\mathbb{F}_l})$$

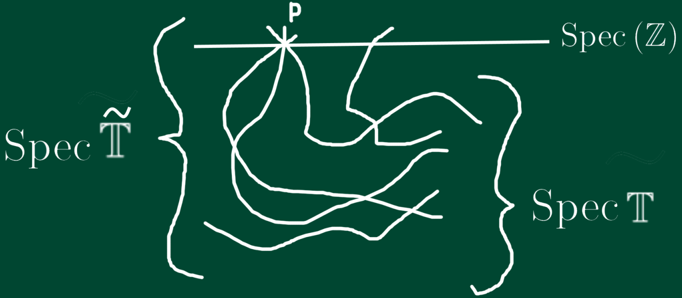
If T_l acts like $l+1$, then this polynomial splits as

$$(X-l)(X-1).$$

This is similar to the representation $(\mathbb{Z}/p\mathbb{Z}) \oplus \mu_p$
This observation will allow us to apply machinery of admissable group schemes

Eisenstein ideal, geometrically

$\widetilde{\mathbb{T}} \subset \mathrm{End}(M_2(\Gamma_0(N)))$ and $\mathbb{T} \subset \mathrm{End}(S_2(\Gamma_0(N)))$



Proposition.

$\mathfrak{a}$ is a proper maximal ideal of $\mathbb{T}$

Proof.

by choice of p, $J_0(N)[p]$ is nontrivial, hence some $V_{f,\lambda}$ contains $\mathbb{Z}/p\mathbb{Z}$ as a sub.

Proposition.

$\mathfrak{a}$ is a proper maximal ideal of $\mathbb{T}$

Proof.

by choice of p, $J_0(N)[p]$ is nontrivial, hence some $V_{f,\lambda}$ contains $\mathbb{Z}/p\mathbb{Z}$ as a sub. We then have that the semisimplified reduction of $V_{f,\lambda}$ is $\mathbb{Z}/p\mathbb{Z} \oplus \mu_p$.

Proposition.

$\mathfrak{a}$ is a proper maximal ideal of $\mathbb{T}$

Proof.

by choice of p, $J_0(N)[p]$ is nontrivial, hence some $V_{f,\lambda}$ contains $\mathbb{Z}/p\mathbb{Z}$ as a sub. We then have that the semisimplified reduction of $V_{f,\lambda}$ is $\mathbb{Z}/p\mathbb{Z} \oplus \mu_p$. Therefore

$$a_l(f) \equiv l + 1 \pmod{\lambda}$$

for $l \neq p, N$.

Proposition.

$\mathfrak{a}$ is a proper maximal ideal of $\mathbb{T}$

Proof.

by choice of p, $J_0(N)[p]$ is nontrivial, hence some $V_{f,\lambda}$ contains $\mathbb{Z}/p\mathbb{Z}$ as a sub. We then have that the semisimplified reduction of $V_{f,\lambda}$ is $\mathbb{Z}/p\mathbb{Z} \oplus \mu_p$. Therefore

$$a_l(f) \equiv l + 1 \pmod{\lambda}$$

for $l \neq p, N$. Therefore, the image of $\mathfrak{a}$ in $\mathcal{O}_f$ is contained in λ, and $\mathfrak{a}$ is a proper ideal. Finally, $0 \neq \mathbb{T}/\mathfrak{a} \subset \mathcal{O}_f/\mathfrak{p}_f$, so $\mathfrak{a}$ is maximal. ∎

Proposition.

$[0] \neq [\infty]$ in A

Proof.

Proposition.

$[0] \neq [\infty]$ in A

Proof.

If $J \subset \mathbb{T}$ is an ideal, we denote $\hat{\mathbb{T}}_J$ for the J-adic completion. Then note that $\hat{\mathbb{T}}_p$ is a direct summand of $\hat{\mathbb{T}}_{\mathfrak{a}}$, denote e the corresponding idempotent.

Proposition.

$[0] \neq [\infty]$ in A

Proof.

If $J \subset \mathbb{T}$ is an ideal, we denote $\hat{\mathbb{T}}_J$ for the J-adic completion. Then note that $\hat{\mathbb{T}}_p$ is a direct summand of $\hat{\mathbb{T}}_{\mathfrak{a}}$, denote e the corresponding idempotent. We have

$$0 \to IJ_0(N)[p^\infty] \to J_0(N)[p^\infty] \to A[p^\infty] \to 0$$

as $\hat{\mathbb{T}}_p$-modules.

Proposition.

$[0] \neq [\infty]$ in A

Proof.

If $J \subset \mathbb{T}$ is an ideal, we denote $\hat{\mathbb{T}}_J$ for the J-adic completion. Then note that $\hat{\mathbb{T}}_p$ is a direct summand of $\hat{\mathbb{T}}_\mathfrak{a}$, denote e the corresponding idempotent. We have

$$0 \to IJ_0(N)[p^\infty] \to J_0(N)[p^\infty] \to A[p^\infty] \to 0$$

as $\hat{\mathbb{T}}_p$-modules. apply e and use that $I_\mathfrak{a} = 0$ by definition of I to get

$$J_0(N)[\mathfrak{a}^\infty] \cong A[\mathfrak{a}^\infty].$$

Proposition.

$[0] \neq [\infty]$ in A

Proof.

If $J \subset \mathbb{T}$ is an ideal, we denote $\hat{\mathbb{T}}_J$ for the J-adic completion. Then note that $\hat{\mathbb{T}}_p$ is a direct summand of $\hat{\mathbb{T}}_{\mathfrak{a}}$, denote e the corresponding idempotent. We have

$$0 \to IJ_0(N)[p^\infty] \to J_0(N)[p^\infty] \to A[p^\infty] \to 0$$

as $\hat{\mathbb{T}}_p$-modules. apply e and use that $I_{\mathfrak{a}} = 0$ by definition of I to get

$$J_0(N)[\mathfrak{a}^\infty] \cong A[\mathfrak{a}^\infty].$$

finally, by choice of p, a multiple of $[0] - [\infty]$ is nontrivial $\mathfrak{a}$-torsion in $J_0(N)$ and so the same is true in A. ■

Overview

Reminders on $J_0(N)$ and the Hecke algebra

Construction of the Eisenstein Quotient

Main argument

Computation of α (the number of $\mathbb{Z}/p\mathbb{Z}$'s)

Computation of δ (the defect at N)

Reminders on admissibility

if B is an abelian variety with good reduction away from N with Néron model $\mathcal{B}$ then $\mathcal{B}[p^n]$ is *preadmissable* over $\mathbb{Z}$ for $p \neq N$. I.e.

Reminders on admissibility

if B is an abelian variety with good reduction away from N with Néron model $\mathcal{B}$ then $\mathcal{B}[p^n]$ is *preadmissable* over $\mathbb{Z}$ for $p \neq N$. I.e.

- seperated, finite type commutative group scheme over $\mathbb{Z}$
- p-power order finite flat over $\mathbb{Z}[1/N]$
- quasifinite flat

Reminders on admissibility

if B is an abelian variety with good reduction away from N with Néron model $\mathcal{B}$ then $\mathcal{B}[p^n]$ is *preadmissable* over $\mathbb{Z}$ for $p \neq N$. I.e.

- seperated, finite type commutative group scheme over $\mathbb{Z}$
- p-power order finite flat over $\mathbb{Z}[1/N]$
- quasifinite flat

Say *admissable* if $\mathcal{B}[p^n]$ satisfies JH(p), i.e. admits a filtration over $\mathbb{Z}[1/N]$ by μ_p's and $\mathbb{Z}/p\mathbb{Z}$'s,

Reminders on admissibility

if B is an abelian variety with good reduction away from N with Néron model $\mathcal{B}$ then $\mathcal{B}[p^n]$ is *preadmissable* over $\mathbb{Z}$ for $p \neq N$. I.e.

- seperated, finite type commutative group scheme over $\mathbb{Z}$
- p-power order finite flat over $\mathbb{Z}[1/N]$
- quasifinite flat

Say *admissable* if $\mathcal{B}[p^n]$ satisfies JH(p), i.e. admits a filtration over $\mathbb{Z}[1/N]$ by μ_p's and $\mathbb{Z}/p\mathbb{Z}$'s, equivalently $\mathcal{B}[p^n](\overline{\mathbb{Q}})$ has a similar filtration by $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules.

$\mathcal{A}[\mathfrak{a}]$ is admissable

$$\mathcal{A}[\mathfrak{a}]/\mathbb{Q} = \bigcap_{\alpha \in \mathfrak{a}} \text{kernel of } \alpha \text{ in } \mathcal{A}[p]/\mathbb{Q}$$

is a finite subgroup scheme of $\mathcal{A}[p]/\mathbb{Q}$. *Define* $\mathcal{A}[\mathfrak{a}]$ to be Zariski closure in $\mathcal{A}[p]$. Still quasifinite flat over $\mathbb{Z}$ and finite over $\mathbb{Z}[1/N]$, hence preadmissable.

$\mathcal{A}[\mathfrak{a}]$ is admissable

$$\mathcal{A}[\mathfrak{a}]/\mathbb{Q} = \bigcap_{\alpha \in \mathfrak{a}} \text{kernel of } \alpha \text{ in } \mathcal{A}[p]/\mathbb{Q}$$

is a finite subgroup scheme of $\mathcal{A}[p]/\mathbb{Q}$. *Define* $\mathcal{A}[\mathfrak{a}]$ to be Zariski closure in $\mathcal{A}[p]$. Still quasifinite flat over $\mathbb{Z}$ and finite over $\mathbb{Z}[1/N]$, hence preadmissable.

Caution

$\mathcal{A}[\mathfrak{a}]/\mathbb{Z}$ is not necessarily the full kernel of $\mathfrak{a}$ in $\mathcal{A}$!

$\mathcal{A}[\mathfrak{a}]$ is admissable

$$\mathcal{A}[\mathfrak{a}]/\mathbb{Q} = \bigcap_{\alpha \in \mathfrak{a}} \text{kernel of } \alpha \text{ in } \mathcal{A}[p]/\mathbb{Q}$$

is a finite subgroup scheme of $\mathcal{A}[p]/\mathbb{Q}$. *Define* $\mathcal{A}[\mathfrak{a}]$ to be Zariski closure in $\mathcal{A}[p]$. Still quasifinite flat over $\mathbb{Z}$ and finite over $\mathbb{Z}[1/N]$, hence preadmissable.

Caution

$\mathcal{A}[\mathfrak{a}]/\mathbb{Z}$ is not necessarily the full kernel of $\mathfrak{a}$ in $\mathcal{A}$!

Lemma

$\mathcal{A}[\mathfrak{a}]$ satisfies JH(p)

Proof.

Proof.

For $l \neq p, N$, Frob_l satisfies $(X-l)(X-1)$ in $\mathrm{Aut}(\mathcal{A}[\mathfrak{a}])$.
Denote W for the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module
$\mathcal{A}[\mathfrak{a}](\overline{\mathbb{Q}}) \oplus (\mathcal{A}[\mathfrak{a}](\overline{\mathbb{Q}}))^*(1)$.

Proof.

For $l \neq p, N$, Frob_l satisfies $(X-l)(X-1)$ in $\mathrm{Aut}(\mathcal{A}[\mathfrak{a}])$. Denote W for the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module $\mathcal{A}[\mathfrak{a}](\overline{\mathbb{Q}}) \oplus (\mathcal{A}[\mathfrak{a}](\overline{\mathbb{Q}}))^*(1)$. It is self-dual, so the characteristic polynomial of Frob_l on W must be of the form

$$(X-l)^d(X-1)^d.$$

Proof.

For $l \neq p, N$, Frob_l satisfies $(X-l)(X-1)$ in $\mathrm{Aut}(\mathcal{A}[\mathfrak{a}])$. Denote W for the $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-module $\mathcal{A}[\mathfrak{a}](\overline{\mathbb{Q}}) \oplus (\mathcal{A}[\mathfrak{a}](\overline{\mathbb{Q}}))^*(1)$. It is self-dual, so the characteristic polynomial of Frob_l on W must be of the form

$$(X-l)^d(X-1)^d.$$

Actually, we can pass to $\mathrm{Gal}(K/\mathbb{Q})$-modules for some $K/\mathbb{Q}$ abelian, hence by Cebotarev all $g \in \mathrm{Gal}(K/\mathbb{Q})$ have the same characteristic polynomial on W^{ss} and $(\mathbb{Z}/p\mathbb{Z})^d \oplus \mu_p^d$. By Brauer-Nesbitt these semisimple representations are isomorphic, so V^{ss} is a sum of $\mathbb{Z}/p\mathbb{Z}$'s and μ_p's ∎

Admissability of the $\mathfrak{a}$-component

Let us denote

$$\mathcal{G}_n := \mathcal{A}[p^n][\mathfrak{a}^\infty] = \mathcal{A}[p^n]_\mathfrak{a} = J_0(N)[p^n]_\mathfrak{a}$$

('$\mathfrak{a}$' component), it is the direct summand of $\mathcal{A}[p^n]$ on which $\hat{\mathbb{T}}_\mathfrak{a}$ acts nontrivially.

Admissability of the $\mathfrak{a}$-component

Let us denote

$$\mathcal{G}_n := \mathcal{A}[p^n][\mathfrak{a}^\infty] = \mathcal{A}[p^n]_\mathfrak{a} = J_0(N)[p^n]_\mathfrak{a}$$

('$\mathfrak{a}$' component), it is the direct summand of $\mathcal{A}[p^n]$ on which $\hat{\mathbb{T}}_\mathfrak{a}$ acts nontrivially.

Proposition

$\mathcal{G}_n$ is admissable

Proof.

Suppose $a_1, \ldots, a_n$ generate $\mathfrak{a}^n/\mathfrak{a}^{n+1}$, then the map $x \mapsto a_1 x \oplus \ldots \oplus a_n x$ yields an injection of $\mathcal{A}[\mathfrak{a}^{(n+1)}]/\mathcal{A}[\mathfrak{a}]$ into $\mathcal{A}[\mathfrak{a}]^n$ as $\mathrm{G}(\overline{\mathbb{Q}}/\mathbb{Q})$-modules. So each $\mathcal{A}[\mathfrak{a}^n]$ satisfies JH(p). $\mathcal{G}_n$ actually lies in $\mathcal{A}[\mathfrak{a}^m]$ for some m. ■

Fundamental inequality

Recall that for any admissable group $G/\mathbb{Z}$, we defined the invariants α (the number of $\mathbb{Z}/p\mathbb{Z}$'s in an admissable filtration) and δ (defect of lengths over $\overline{\mathbb{Q}}$ and $\overline{\mathbb{F}}_N$), we showed

$$h^1(G) - h^0(G) \leq \delta(G) - \alpha(G)$$

Fundamental inequality

Recall that for any admissable group $G/\mathbb{Z}$, we defined the invariants α (the number of $\mathbb{Z}/p\mathbb{Z}$'s in an admissable filtration) and δ (defect of lengths over $\overline{\mathbb{Q}}$ and $\overline{\mathbb{F}}_N$), we showed

$$h^1(G) - h^0(G) \leq \delta(G) - \alpha(G)$$

Later we will show that for $d = \mathrm{rank}_{\mathbb{Z}_p} \hat{\mathbb{T}}_{\mathfrak{a}}$ we have

Lemma

$$\alpha(\mathcal{G}_n) = nd + O(1) \quad \text{and} \quad \delta(\mathcal{G}_n) = nd + O(1)$$

Deduction from computations of α and δ

Theorem

$A(\mathbb{Q})$ has rank 0.

Proof

Deduction from computations of α and δ

Theorem

$A(\mathbb{Q})$ has rank 0.

Proof

Denote $\mathcal{H}_n = \mathcal{A}^\circ[p^n]_{\mathfrak{a}}$. Then

$$\begin{aligned} h^1(\mathcal{H}_n) - h^0(\mathcal{H}_n) &\leq \delta(\mathcal{H}_n) - \alpha(\mathcal{H}_n) \\ &= (\delta(\mathcal{G}_n) + O(1)) - \alpha(\mathcal{G}_n) \\ &= O(1) \end{aligned}$$

Deduction from computations of α and δ

Theorem

$A(\mathbb{Q})$ has rank 0.

Proof

Denote $\mathcal{H}_n = \mathcal{A}^\circ[p^n]_\mathfrak{a}$. Then

$$\begin{aligned} h^1(\mathcal{H}_n) - h^0(\mathcal{H}_n) &\leq \delta(\mathcal{H}_n) - \alpha(\mathcal{H}_n) \\ &= (\delta(\mathcal{G}_n) + O(1)) - \alpha(\mathcal{G}_n) \\ &= O(1) \end{aligned}$$

note that $\mathrm{H}^0_{fppf}(\mathrm{Spec}\,(\mathbb{Z}), \mathcal{H}_n) \subset \mathcal{A}(\mathbb{Z})[p^n] = A(\mathbb{Q})[p^n]$ has bounded size by Mordell-Weil.

Proof (continued).

The Kummer sequence in fppf cohomology yields an injection

$$\mathcal{A}^\circ(\mathbb{Z}) \otimes \mathbb{Z}_p \to \varprojlim \mathrm{H}^1_{fppf}(\mathrm{Spec}\,(\mathbb{Z}), \mathcal{A}^\circ[p^n])$$

tensoring by $\mathbb{T}$ and apply the idempotent e:

$$\mathcal{A}^\circ(\mathbb{Z}) \otimes_{\mathbb{T}} \hat{\mathbb{T}}_{\mathfrak{a}} \to \varprojlim \mathrm{H}^1_{fppf}(\mathrm{Spec}\,(\mathbb{Z}), \mathcal{H}_n)$$

Proof (continued).

The Kummer sequence in fppf cohomology yields an injection

$$\mathcal{A}^\circ(\mathbb{Z}) \otimes \mathbb{Z}_p \to \varprojlim \mathrm{H}^1_{fppf}(\mathrm{Spec}\,(\mathbb{Z}), \mathcal{A}^\circ[p^n])$$

tensoring by $\mathbb{T}$ and apply the idempotent e:

$$\mathcal{A}^\circ(\mathbb{Z}) \otimes_{\mathbb{T}} \hat{\mathbb{T}}_{\mathfrak{a}} \to \varprojlim \mathrm{H}^1_{fppf}(\mathrm{Spec}\,(\mathbb{Z}), \mathcal{H}_n)$$

As $\mathcal{A}^0(\mathbb{Z})$ is of finite index in $\mathcal{A}(\mathbb{Z}) = A(\mathbb{Q})$, the conclusion is that $A(\mathbb{Q}) \otimes_{\mathbb{T}} \hat{\mathbb{T}}_a$ is finite.

Proof (continued).

The Kummer sequence in fppf cohomology yields an injection

$$\mathcal{A}^{\circ}(\mathbb{Z}) \otimes \mathbb{Z}_p \to \lim_{\leftarrow} \mathrm{H}^1_{fppf}(\mathrm{Spec}\,(\mathbb{Z}), \mathcal{A}^{\circ}[p^n])$$

tensoring by $\mathbb{T}$ and apply the idempotent e:

$$\mathcal{A}^{\circ}(\mathbb{Z}) \otimes_{\mathbb{T}} \hat{\mathbb{T}}_{\mathfrak{a}} \to \lim_{\leftarrow} \mathrm{H}^1_{fppf}(\mathrm{Spec}\,(\mathbb{Z}), \mathcal{H}_n)$$

As $\mathcal{A}^0(\mathbb{Z})$ is of finite index in $\mathcal{A}(\mathbb{Z}) = A(\mathbb{Q})$, the conclusion is that $A(\mathbb{Q}) \otimes_{\mathbb{T}} \hat{\mathbb{T}}_a$ is finite.
$A_f(\mathbb{Q}) = \mathcal{A}(\mathbb{Q})/\mathfrak{p}_f A(\mathbb{Q})$ is a finitely generated module over $\mathcal{O}_f$, so if we take completions at $\mathfrak{a}$ we see that $A_f(\mathbb{Q})$ is finite.
We conclude by the isogeny $A \to \prod_{\mathfrak{p}_f \subset \mathfrak{a}} A/\mathfrak{p}_f A$. ■

Overview

Reminders on $J_0(N)$ and the Hecke algebra

Construction of the Eisenstein Quotient

Main argument

Computation of α (the number of $\mathbb{Z}/p\mathbb{Z}$'s)

Computation of δ (the defect at N)

Recall $\mathcal{G}_n = \mathcal{A}[p^n]_{\mathfrak{a}}$, and we set $d = \mathrm{rank}_{\mathbb{Z}_p} \hat{\mathbb{T}}_{\mathfrak{a}}$.

Recall $\mathcal{G}_n = \mathcal{A}[p^n]_{\mathfrak{a}}$, and we set $d = \mathrm{rank}_{\mathbb{Z}_p} \hat{\mathbb{T}}_{\mathfrak{a}}$.

length of $\mathcal{G}_n$

$\mathrm{len}(\mathcal{G}_n) = 2nd + O(1)$

Proof.

Let $\mathcal{G} = \mathcal{A}[p^\infty]_{\mathfrak{a}}$, this is a p-divisible group, with p-adic Tate module $V_p(\mathcal{G}) = T_p(\mathcal{G}) \otimes_{\mathbb{Q}} \mathbb{Q}_p$ free of rank 2 over $\hat{\mathbb{T}}_{\mathfrak{a}}[1/p]$ as p is ordinary.

Recall $\mathcal{G}_n = \mathcal{A}[p^n]_{\mathfrak{a}}$, and we set $d = \mathrm{rank}_{\mathbb{Z}_p} \hat{\mathbb{T}}_{\mathfrak{a}}$.

length of $\mathcal{G}_n$

$\mathrm{len}(\mathcal{G}_n) = 2nd + O(1)$

Proof.

Let $\mathcal{G} = \mathcal{A}[p^\infty]_{\mathfrak{a}}$, this is a p-divisible group, with p-adic Tate module $V_p(\mathcal{G}) = T_p(\mathcal{G}) \otimes_{\mathbb{Q}} \mathbb{Q}_p$ free of rank 2 over $\hat{\mathbb{T}}_{\mathfrak{a}}[1/p]$ as p is ordinary. Therefore $T_p(\mathcal{G})$ contains a rank 2 free $\hat{\mathbb{T}}_{\mathfrak{a}}$-submodule T'.

Recall $\mathcal{G}_n = \mathcal{A}[p^n]_{\mathfrak{a}}$, and we set $d = \mathrm{rank}_{\mathbb{Z}_p} \hat{\mathbb{T}}_{\mathfrak{a}}$.

length of $\mathcal{G}_n$

$\mathrm{len}(\mathcal{G}_n) = 2nd + O(1)$

Proof.

Let $\mathcal{G} = \mathcal{A}[p^\infty]_{\mathfrak{a}}$, this is a p-divisible group, with p-adic Tate module $V_p(\mathcal{G}) = T_p(\mathcal{G}) \otimes_{\mathbb{Q}} \mathbb{Q}_p$ free of rank 2 over $\hat{\mathbb{T}}_{\mathfrak{a}}[1/p]$ as p is ordinary. Therefore $T_p(\mathcal{G})$ contains a rank 2 free $\hat{\mathbb{T}}_{\mathfrak{a}}$-submodule T'. Hence

$$\begin{aligned}
\mathrm{len}(\mathcal{G}_n) &= \mathrm{len}(\mathcal{G}[p^n]) \\
&= \mathrm{len}(T_p(\mathcal{G})/p^n T_p(\mathcal{G})) \\
&= \mathrm{len}(T'/p^n T') + O(1) \\
&= 2nd + O(1)
\end{aligned}$$

∎

idea: descent selfduality $J_0(N)$ to $\mathfrak{a}$-component

$\alpha(\mathcal{G}_n) = nd + O(1)$

idea: descent selfduality $J_0(N)$ to $\mathfrak{a}$-component

$\alpha(\mathcal{G}_n) = nd + O(1)$

Before we showed that $\mathcal{A}_{\mathfrak{a}} = J_0(N)_{\mathfrak{a}}$, hence
$\mathcal{G}_n = J_0N[p^n]_{\mathfrak{a}} = eJ_0(N)[p^n]$.

idea: descent selfduality $J_0(N)$ to $\mathfrak{a}$-component

$\alpha(\mathcal{G}_n) = nd + O(1)$

Before we showed that $\mathcal{A}_\mathfrak{a} = J_0(N)_\mathfrak{a}$, hence $\mathcal{G}_n = J_0N[p^n]_\mathfrak{a} = eJ_0(N)[p^n]$. Let $x \in J_0(N)[p^n]$. As e is self-adjoint in the Weil paring,

$$\langle ex, (1-e)x \rangle = \langle e(1-e)x, x \rangle = 0$$

so this implies the Weil paring restricts to a pairing on $\mathcal{G}_n$, which is perfect as it is perfect on $J_0(N)[p^n]$.

idea: descent selfduality $J_0(N)$ to $\mathfrak{a}$-component

$\alpha(\mathcal{G}_n) = nd + O(1)$

Before we showed that $\mathcal{A}_{\mathfrak{a}} = J_0(N)_{\mathfrak{a}}$, hence $\mathcal{G}_n = J_0 N[p^n]_{\mathfrak{a}} = eJ_0(N)[p^n]$. Let $x \in J_0(N)[p^n]$. As e is self-adjoint in the Weil paring,

$$\langle ex, (1-e)x \rangle = \langle e(1-e)x, x \rangle = 0$$

so this implies the Weil paring restricts to a pairing on $\mathcal{G}_n$, which is perfect as it is perfect on $J_0(N)[p^n]$.
Hence $\mathcal{G}_n$ is Cartier selfdual, thus
$\alpha = 1/2 \operatorname{len}(\mathcal{G}_n) = nd + O(1)$. ■

Overview

Reminders on $J_0(N)$ and the Hecke algebra

Construction of the Eisenstein Quotient

Main argument

Computation of α (the number of $\mathbb{Z}/p\mathbb{Z}$'s)

Computation of δ (the defect at N)

First we study how the inertia I at N acts on the p-adic Tate module.

Lemma.

for any abelian variety A with good reduction at p,

$$V_p(A)^I = V_p(\mathcal{A}_{\mathbb{F}_N})$$

First we study how the inertia I at N acts on the p-adic Tate module.

Lemma.

for any abelian variety A with good reduction at p,

$$V_p(A)^I = V_p(\mathcal{A}_{\mathbb{F}_N})$$

Proof.

Note $\mathcal{A}[p^n]$ is étale, and $\mathbb{Z}_N^{unr}$ is strictly Henselian, so

$$\mathcal{A}[p^n](\mathbb{Z}_N^{\mathrm{unr}}) \twoheadrightarrow \mathcal{A}[p^n](\overline{\mathbb{F}}_N),$$

First we study how the inertia I at N acts on the p-adic Tate module.

Lemma.

for any abelian variety A with good reduction at p,

$$V_p(A)^I = V_p(\mathcal{A}_{\mathbb{F}_N})$$

Proof.

Note $\mathcal{A}[p^n]$ is étale, and $\mathbb{Z}_N^{unr}$ is strictly Henselian, so

$$\mathcal{A}[p^n](\mathbb{Z}_N^{\mathrm{unr}}) \twoheadrightarrow \mathcal{A}[p^n](\overline{\mathbb{F}}_N),$$

By the Neron mapping property $\mathcal{A}[p^n](\mathbb{Z}_N^{\mathrm{unr}}) = \mathcal{A}[p^n](\mathbb{Q}_N^{\mathrm{unr}})$.

First we study how the inertia I at N acts on the p-adic Tate module.

Lemma.

for any abelian variety A with good reduction at p,

$$V_p(A)^I = V_p(\mathcal{A}_{\mathbb{F}_N})$$

Proof.

Note $\mathcal{A}[p^n]$ is étale, and $\mathbb{Z}_N^{unr}$ is strictly Henselian, so

$$\mathcal{A}[p^n](\mathbb{Z}_N^{\mathrm{unr}}) \twoheadrightarrow \mathcal{A}[p^n](\overline{\mathbb{F}}_N),$$

By the Neron mapping property $\mathcal{A}[p^n](\mathbb{Z}_N^{\mathrm{unr}}) = \mathcal{A}[p^n](\mathbb{Q}_N^{\mathrm{unr}})$. In general, for finite étale group schemes over $\mathbb{Z}_N$ we have $G(\overline{\mathbb{Q}_N}) = G(\overline{\mathbb{F}}_N)$ ∎

How to compute δ for $\mathcal{A}[p^n]$

As A has completely toric reduction at N, so

$$(V_p A)^I = V_p(\mathbb{G}_{m,\mathbb{F}_N}^{\dim A})$$

is a $\dim A$-dimensional p-adic representation.

How to compute δ for $\mathcal{A}[p^n]$

As A has completely toric reduction at N, so

$$(V_p A)^I = V_p(\mathbb{G}_{m,\mathbb{F}_N}^{\dim A})$$

is a $\dim A$-dimensional p-adic representation.

$$\begin{aligned}\delta(\mathcal{A}[p^n]) &= \mathrm{len}(\mathcal{A}[p^n]) - \mathrm{len}(\mathcal{A}[p^n]_{\mathbb{F}_N}) \\ &= 2n\dim(A) - n\dim A \\ &= n\dim A\end{aligned}$$

Passing to $\mathfrak{a}$

applying the idempotent e, we get

Corollary (of last lemma)

$$\mathcal{G}_n(\overline{\mathbb{F}}_N) = \mathcal{G}_n(\overline{\mathbb{Q}}_N)^I$$

Passing to $\mathfrak{a}$

applying the idempotent e, we get

Corollary (of last lemma)

$$\mathcal{G}_n(\overline{\mathbb{F}}_N) = \mathcal{G}_n(\overline{\mathbb{Q}}_N)^I$$

Proposition.

If $U \subset V_p A$ is any summand, we have $\dim(U^I) = 1/2 \dim(U)$. This applies in particular to the Tate module $V_p\mathcal{G}$ of the p-divisible group $\mathcal{G} = \mathcal{A}[p^\infty]_{\mathfrak{a}} = eV_p(A)$

Passing to $\mathfrak{a}$

applying the idempotent e, we get

Corollary (of last lemma)

$$\mathcal{G}_n(\overline{\mathbb{F}}_N) = \mathcal{G}_n(\overline{\mathbb{Q}}_N)^I$$

Proposition.

If $U \subset V_pA$ is any summand, we have $\dim(U^I) = 1/2\dim(U)$. This applies in particular to the Tate module $V_p\mathcal{G}$ of the p-divisible group $\mathcal{G} = \mathcal{A}[p^\infty]_{\mathfrak{a}} = eV_p(A)$

Proof.

Say $U \oplus U' = V$. Clearly $U^I \oplus U'^I = V^I$ and $\dim V_pA^I = 1/2\dim V_pA$,

Passing to $\mathfrak{a}$

applying the idempotent e, we get

Corollary (of last lemma)

$$\mathcal{G}_n(\overline{\mathbb{F}}_N) = \mathcal{G}_n(\overline{\mathbb{Q}}_N)^I$$

Proposition.

If $U \subset V_pA$ is any summand, we have $\dim(U^I) = 1/2\dim(U)$. This applies in particular to the Tate module $V_p\mathcal{G}$ of the p-divisible group $\mathcal{G} = \mathcal{A}[p^\infty]_{\mathfrak{a}} = eV_p(A)$

Proof.

Say $U \oplus U' = V$. Clearly $U^I \oplus U'^I = V^I$ and $\dim V_pA^I = 1/2\dim V_pA$, so suffices to show the claim $\dim U^I \geq 1/2 \dim U$ (and similar for U').

Proof. (continued)

- By semistability inertia acts unipotently on U, and wild inertia P acts trivally, as pro-N. also I/P is pro-cyclic, say topologically generated by g, have $U^I = U^g$

Proof. (continued)

- By semistability inertia acts unipotently on U, and wild inertia P acts trivally, as pro-N. also I/P is pro-cyclic, say topologically generated by g, have $U^I = U^g$
- All $V_{f,\lambda}$ for λ above p in K_f, $\mathfrak{p}_f \subset \mathfrak{a}$ are 2-dimensional, $(g-1)^2$ on V_pA.

Proof. (continued)

- By semistability inertia acts unipotently on U, and wild inertia P acts trivally, as pro-N. also I/P is pro-cyclic, say topologically generated by g, have $U^I = U^g$
- All $V_{f,\lambda}$ for λ above p in K_f, $\mathfrak{p}_f \subset \mathfrak{a}$ are 2-dimensional, $(g-1)^2$ on V_pA.

Therefore

$$\dim(U^I) = \dim(U^g) \geq \dim((g-1)U) \geq \frac{1}{2}\dim(U)$$

∎

Proof. (continued)

- By semistability inertia acts unipotently on U, and wild inertia P acts trivally, as pro-N. also I/P is pro-cyclic, say topologically generated by g, have $U^I = U^g$
- All $V_{f,\lambda}$ for λ above p in K_f, $\mathfrak{p}_f \subset \mathfrak{a}$ are 2-dimensional, $(g-1)^2$ on V_pA.

Therefore

$$\dim(U^I) = \dim(U^g) \geq \dim((g-1)U) \geq \frac{1}{2}\dim(U)$$

∎

Remark

More generally, Grothendieck's orthogonality theorem implies that inertia acts unipotently on the Tate module of any semistable abelian variety in 2 steps, i.e. $(g-1)^2 = 0$ holds.

Computing inertia invariants

Computing inertia invariants

Lemma

$\mathrm{len}(\mathcal{G}_n(\overline{\mathbb{Q}}_N)^I) = nd + O(1)$

Computing inertia invariants

Lemma

$\mathrm{len}(\mathcal{G}_n(\overline{\mathbb{Q}}_N)^I) = nd + O(1)$

Proof.

Let $T = T_p\mathcal{G}$ and $V = V_p\mathcal{G}$. Galois cohomology gives

$$0 \to T^I/p^nT^I \to (T/p^nT)^I \to \mathrm{H}^1(I,T)[p^n] \to 0$$

and $\mathrm{H}^1(I,T)$ is a finitely generated $\mathbb{Z}_p$-module.

Computing inertia invariants

Lemma

$\mathrm{len}(\mathcal{G}_n(\overline{\mathbb{Q}}_N)^I) = nd + O(1)$

Proof.

Let $T = T_p\mathcal{G}$ and $V = V_p\mathcal{G}$. Galois cohomology gives

$$0 \to T^I/p^nT^I \to (T/p^nT)^I \to \mathrm{H}^1(I,T)[p^n] \to 0$$

and $\mathrm{H}^1(I,T)$ is a finitely generated $\mathbb{Z}_p$-module. Hence $\mathrm{len}((T/{}^nT)^I) = \mathrm{len}(T^I/p^nT^I) + O(1)$.

Computing inertia invariants

Lemma

$\mathrm{len}(\mathcal{G}_n(\overline{\mathbb{Q}}_N)^I) = nd + O(1)$

Proof.

Let $T = T_p\mathcal{G}$ and $V = V_p\mathcal{G}$. Galois cohomology gives

$$0 \to T^I/p^nT^I \to (T/p^nT)^I \to \mathrm{H}^1(I,T)[p^n] \to 0$$

and $\mathrm{H}^1(I,T)$ is a finitely generated $\mathbb{Z}_p$-module. Hence $\mathrm{len}((T/^nT)^I) = \mathrm{len}(T^I/p^nT^I) + O(1)$.
Now using the previous lemma,

$$\mathrm{len}(T^I/p^nT^I) = \dim(V^I) = \frac{1}{2}\dim V = nd$$

For the last step, recall V is a free rank 2 $\hat{\mathbb{T}}_a[1/p]$-module. ∎

Computation of δ

Finally,

$$\begin{aligned}\delta(\mathcal{G}_n) &= \operatorname{len}(\mathcal{G}_n) - \operatorname{len}((\mathcal{G}_n)_{\overline{\mathbb{F}}_N}) \\ &= 2nd - \operatorname{len}(\mathcal{G}_n(\overline{\mathbb{Q}}_N)^I) + O(1) \\ &= nd + O(1)\end{aligned}$$