Constructing Unramified Extensions of $\mathbb{Q}(\mu_p)$

Ricky Magner

October 29, 2020

Overview

Table of Contents

Notation

- Fix a prime p. Let A be the class group of $\mathbb{Q}(\mu_p)$. Set $C = A/A^p$.

Notation

- Fix a prime p. Let A be the class group of $\mathbb{Q}(\mu_p)$. Set $C = A/A^p$.
- Let $\Delta = \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$, and let $\chi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \Delta \to \mathbb{F}_p^\times$ be the mod p cyclotomic character.

Notation

- Fix a prime p. Let A be the class group of $\mathbb{Q}(\mu_p)$. Set $C = A/A^p$.
- Let $\Delta = \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$, and let $\chi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \Delta \to \mathbb{F}_p^\times$ be the mod p cyclotomic character.
- Then C decomposes as $\oplus_i C(\chi^i)$ where $C(\chi^i)$ is the χ^i-isotypic component of C as a Galois module.

Notation

- Fix a prime p. Let A be the class group of $\mathbb{Q}(\mu_p)$. Set $C = A/A^p$.
- Let $\Delta = \mathrm{Gal}(\mathbb{Q}(\mu_p)/\mathbb{Q})$, and let $\chi : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \Delta \to \mathbb{F}_p^\times$ be the mod p cyclotomic character.
- Then C decomposes as $\oplus_i C(\chi^i)$ where $C(\chi^i)$ is the χ^i-isotypic component of C as a Galois module.
- Let B_k be the kth Bernoulli number, e.g. $B_k = -k\zeta(1-k)$.

The Theorem

- Let $2 \leq k \leq p - 3$ be even.

The Theorem

- Let $2 \leq k \leq p-3$ be even.

Theorem (Ribet-Herbrand)

$p \mid B_k$ if and only if $C(\chi^{1-k}) \neq 0$.

The Theorem

- Let $2 \leq k \leq p - 3$ be even.

Theorem (Ribet-Herbrand)

$p \mid B_k$ if and only if $C(\chi^{1-k}) \neq 0$.

- The "if" direction is due to Herbrand; follows from Stickelberger's theorem.

The Theorem

- Let $2 \leq k \leq p-3$ be even.

Theorem (Ribet-Herbrand)

$p \mid B_k$ if and only if $C(\chi^{1-k}) \neq 0$.

- The "if" direction is due to Herbrand; follows from Stickelberger's theorem.
- The "only if" direction is a corollary to Vandiver's conjecture that p does not divide the class number of $\mathbb{Q}(\mu_p)^+$, but Ribet gives an unconditional proof.

CFT Translation

- The goal: if $p \mid B_k$, then $C(\chi^{1-k}) \neq 0$. By CFT, this is equivalent to showing:

CFT Translation

- The goal: if $p \mid B_k$, then $C(\chi^{1-k}) \neq 0$. By CFT, this is equivalent to showing:

Theorem (1.2)

Suppose $p \mid B_k$. Then there exists a Galois extension $E/\mathbb{Q}$ with group G with the properties:

CFT Translation

- The goal: if $p \mid B_k$, then $C(\chi^{1-k}) \neq 0$. By CFT, this is equivalent to showing:

Theorem (1.2)

Suppose $p \mid B_k$. Then there exists a Galois extension $E/\mathbb{Q}$ with group G with the properties:

a. *$E/\mathbb{Q}(\mu_p)$ is unramified abelian with group H of type $(p, \ldots, p)$, i.e. killed by p.*

CFT Translation

- The goal: if $p \mid B_k$, then $C(\chi^{1-k}) \neq 0$. By CFT, this is equivalent to showing:

Theorem (1.2)

Suppose $p \mid B_k$. Then there exists a Galois extension $E/\mathbb{Q}$ with group G with the properties:

a. *$E/\mathbb{Q}(\mu_p)$ is unramified abelian with group H of type $(p, \dots, p)$, i.e. killed by p.*
b. *For $\sigma \in G, \tau \in H$,*
$$\sigma\tau\sigma^{-1} = \chi(\sigma)^{1-k}\tau.$$

CFT Translation

- The goal: if $p \mid B_k$, then $C(\chi^{1-k}) \neq 0$. By CFT, this is equivalent to showing:

Theorem (1.2)

Suppose $p \mid B_k$. Then there exists a Galois extension $E/\mathbb{Q}$ with group G with the properties:

a. *$E/\mathbb{Q}(\mu_p)$ is unramified abelian with group H of type $(p, \ldots, p)$, i.e. killed by p.*
b. *For $\sigma \in G, \tau \in H$,*
$$\sigma\tau\sigma^{-1} = \chi(\sigma)^{1-k}\tau.$$

- Let $\mathbb{Q}(\mu_p^{\otimes(1-k)})$ be the unique subfield of $\mathbb{Q}(\mu_p)$ of degree $(p-1)/(p-1, k-1)$ over $\mathbb{Q}$. Ribet shows a stronger version of (1.2) with this field in place of $\mathbb{Q}(\mu_p)$.

Galois Representation

To prove (1.2), Ribet defers to a more representation theoretic theorem.

Galois Representation

To prove (1.2), Ribet defers to a more representation theoretic theorem.

Theorem (1.3)

If $p \mid B_k$, then there exists $\mathbb{F}/\mathbb{F}_p$ finite and a continuous

$$\overline{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F})$$

such that

Galois Representation

To prove (1.2), Ribet defers to a more representation theoretic theorem.

Theorem (1.3)

If $p \mid B_k$, then there exists $\mathbb{F}/\mathbb{F}_p$ finite and a continuous

$$\overline{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F})$$

such that

- i $\overline{\rho}$ *is unramified for $\ell \neq p$;*

Galois Representation

To prove (1.2), Ribet defers to a more representation theoretic theorem.

Theorem (1.3)

If $p \mid B_k$, then there exists $\mathbb{F}/\mathbb{F}_p$ finite and a continuous

$$\overline{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F})$$

such that

i. *$\overline{\rho}$ is unramified for $\ell \neq p$;*
ii. *$\overline{\rho}$ is an extension of χ^{k-1} by 1 (im $\approx$ upper triangular);*

Galois Representation

To prove (1.2), Ribet defers to a more representation theoretic theorem.

Theorem (1.3)

If $p \mid B_k$, then there exists $\mathbb{F}/\mathbb{F}_p$ finite and a continuous

$$\overline{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F})$$

such that

- i $\overline{\rho}$ *is unramified for* $\ell \neq p$*;*
- ii $\overline{\rho}$ *is an extension of* χ^{k-1} *by* 1 *(im* $\approx$ *upper triangular);*
- iii *im(*$\overline{\rho}$*) has order divisible by p, so* $\overline{\rho}$ *is not diagonalizable;*

Galois Representation

To prove (1.2), Ribet defers to a more representation theoretic theorem.

Theorem (1.3)

If $p \mid B_k$, then there exists $\mathbb{F}/\mathbb{F}_p$ finite and a continuous

$$\overline{\rho} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F})$$

such that

- i $\overline{\rho}$ *is unramified for* $\ell \neq p$;
- ii $\overline{\rho}$ *is an extension of* χ^{k-1} *by* 1 *(im ≈ upper triangular);*
- iii *im*($\overline{\rho}$) *has order divisible by p, so* $\overline{\rho}$ *is not diagonalizable;*
- iv *for D a decomposition group for p in* $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$, $\overline{\rho}|_D$ *is diagonalizable, i.e. im*($\overline{\rho}|_D$) *is not divisible by p.*

(1.3) $\implies$ (1.2)

- Let $\overline{\rho}$ be as in (1.3) and set $E = \overline{\mathbb{Q}}^{\ker \overline{\rho}}$, so $E/\mathbb{Q}$ is Galois with group $\mathrm{im}(\overline{\rho})$ of type $(p, \ldots, p)$ over $\mathbb{Q}(\mu_p^{\otimes(1-k)})$.

$(1.3) \implies (1.2)$

- Let $\overline{\rho}$ be as in (1.3) and set $E = \overline{\mathbb{Q}}^{\ker \overline{\rho}}$, so $E/\mathbb{Q}$ is Galois with group $\mathrm{im}(\overline{\rho})$ of type $(p, \ldots, p)$ over $\mathbb{Q}(\mu_p^{\otimes(1-k)})$.
- By (i), $E/\mathbb{Q}$ is unramified away from p, and by (iii), $E/\mathbb{Q}(\mu_p^{\otimes(1-k)})$ is nontrivial. By (iv), this extension is unramified at p, so it is unramified everywhere.

$(1.3) \implies (1.2)$

- Let $\overline{\rho}$ be as in (1.3) and set $E = \overline{\mathbb{Q}}^{\ker \overline{\rho}}$, so $E/\mathbb{Q}$ is Galois with group $\mathrm{im}(\overline{\rho})$ of type $(p, \ldots, p)$ over $\mathbb{Q}(\mu_p^{\otimes(1-k)})$.
- By (i), $E/\mathbb{Q}$ is unramified away from p, and by (iii), $E/\mathbb{Q}(\mu_p^{\otimes(1-k)})$ is nontrivial. By (iv), this extension is unramified at p, so it is unramified everywhere.
- The conjugation formula follows from (ii) and an analogous formula on the level of upper triangular matrices, used to represent the image of $\overline{\rho}$.

Anatomy of the Paper

- Section 1: Introduction
- Section 2: Lemma (2.1) on mod p representations
- Section 3: Creating a cuspform f with specific congruence conditions
- Section 4: Construction of $\overline{\rho}$ from f

Table of Contents

Divisibility of B_k

- Let $E_k = -B_k/2k + \sum \sigma_{k-1}(n)q^n$ be the Eisenstein series of weight k.

Divisibility of B_k

- Let $E_k = -B_k/2k + \sum \sigma_{k-1}(n)q^n$ be the Eisenstein series of weight k.
- The inspiration of this bridge from $p \mid B_k$ to creating $\overline{\rho}$ comes from observing that under this assumption, E_k looks like a cuspform mod p.

Divisibility of B_k

- Let $E_k = -B_k/2k + \sum \sigma_{k-1}(n)q^n$ be the Eisenstein series of weight k.
- The inspiration of this bridge from $p \mid B_k$ to creating $\overline{\rho}$ comes from observing that under this assumption, E_k looks like a cuspform mod p.
- Then one may hope that $E_k \equiv f$ mod p for some genuine cuspform f that lifts and produces a Galois representation with the desired properties since the Fourier coefficients of E_k match the values traces of Frobenius on $\mathbf{1} \oplus \chi^{k-1}$.

The Cuspform

- To create $\overline{\rho}$ as in Theorem (1.3), Ribet creates a Hecke eigenform and produces from it an associated Galois representation.

The Cuspform

- To create $\overline{\rho}$ as in Theorem (1.3), Ribet creates a Hecke eigenform and produces from it an associated Galois representation.

Theorem (3.7)

There exists $f = \sum a_n q^n$ a normalized cuspidal eigenform of weight 2 and level $\Gamma_1(p)$ of type ε satisfying

$$a_\ell \equiv \sigma_{k-1}(\ell) = 1 + \ell^{k-1} \equiv 1 + \varepsilon(\ell)\ell \mod \mathfrak{p}$$

where $\mathfrak{p}$ divides p in K, the field generated by the a_n's.

The Residual Representation

- From f as above, Ribet creates ρ_f, a p-adic representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.

The Residual Representation

- From f as above, Ribet creates ρ_f, a p-adic representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.
- The congruences above then imply the reduction mod p is an extension of χ^{k-1} by $\mathbf{1}$, and the representation is unramified away from p since it arises from a modular form for $\Gamma_1(p)$. This establishes (1.3) (i) and (ii) for $\overline{\rho}_f$.

The Residual Representation

- From f as above, Ribet creates ρ_f, a p-adic representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.
- The congruences above then imply the reduction mod p is an extension of χ^{k-1} by $\mathbf{1}$, and the representation is unramified away from p since it arises from a modular form for $\Gamma_1(p)$. This establishes (1.3) (i) and (ii) for $\overline{\rho}_f$.
- (1.3)(iii) follows from (2.1) and simplicity of ρ_f.

The Residual Representation

- From f as above, Ribet creates ρ_f, a p-adic representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$.
- The congruences above then imply the reduction mod p is an extension of χ^{k-1} by $\mathbf{1}$, and the representation is unramified away from p since it arises from a modular form for $\Gamma_1(p)$. This establishes (1.3) (i) and (ii) for $\overline{\rho}_f$.
- (1.3)(iii) follows from (2.1) and simplicity of ρ_f.
- (1.3)(iv) comes from a geometric argument involving Raynaud's classification of group schemes of type $(p, \ldots, p)$.

Table of Contents

Setup

- Let $f, K, \mathfrak{p}$ be as in (3.7), so $f = \sum a_n q^n$, $K = \mathbb{Q}(\{a_n\})$, and $f \equiv E_k \bmod \mathfrak{p}$.

Setup

- Let $f, K, \mathfrak{p}$ be as in (3.7), so $f = \sum a_n q^n$, $K = \mathbb{Q}(\{a_n\})$, and $f \equiv E_k \bmod \mathfrak{p}$.
- Let $K_\mathfrak{p}$ be the completion of K at $\mathfrak{p}$, with ring of integers $\mathcal{O}_\mathfrak{p}$. Let π be a uniformizer of $\mathcal{O}_\mathfrak{p}$.

Setup

- Let $f, K, \mathfrak{p}$ be as in (3.7), so $f = \sum a_n q^n$, $K = \mathbb{Q}(\{a_n\})$, and $f \equiv E_k \bmod \mathfrak{p}$.
- Let $K_\mathfrak{p}$ be the completion of K at $\mathfrak{p}$, with ring of integers $\mathcal{O}_\mathfrak{p}$. Let π be a uniformizer of $\mathcal{O}_\mathfrak{p}$.
- Write $\mathbb{F}$ for $\mathcal{O}_\mathfrak{p}/\mathfrak{p}$.

Shimura's Construction

Shimura showed there exists an abelian variety $A = A_f/\mathbb{Q}$ associated to f, with the following properties:

Shimura's Construction

Shimura showed there exists an abelian variety $A = A_f/\mathbb{Q}$ associated to f, with the following properties:

1. $\dim(A) = [K : \mathbb{Q}]$, and $K \subseteq \mathrm{End}^0(A_{\mathbb{Q}})$, so

$$V_{\mathfrak{p}} := V_p(A) \otimes_{K \otimes \mathbb{Q}_p} K_{\mathfrak{p}}$$

is a 2-dimensional $K_{\mathfrak{p}}$ vector space with a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action.

Shimura's Construction

Shimura showed there exists an abelian variety $A = A_f/\mathbb{Q}$ associated to f, with the following properties:

1. $\dim(A) = [K : \mathbb{Q}]$, and $K \subseteq \mathrm{End}^0(A_{\overline{\mathbb{Q}}})$, so

$$V_{\mathfrak{p}} := V_p(A) \otimes_{K \otimes \mathbb{Q}_p} K_{\mathfrak{p}}$$

   is a 2-dimensional $K_{\mathfrak{p}}$ vector space with a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action.
2. A arises as a quotient of $J_1(p)$, so $V_{\mathfrak{p}}$ is unramified at $\ell \neq p$.

Shimura's Construction

Shimura showed there exists an abelian variety $A = A_f/\mathbb{Q}$ associated to f, with the following properties:

1. $\dim(A) = [K : \mathbb{Q}]$, and $K \subseteq \mathrm{End}^0(A_{\mathbb{Q}})$, so
$$V_{\mathfrak{p}} := V_p(A) \otimes_{K\otimes\mathbb{Q}_p} K_{\mathfrak{p}}$$
is a 2-dimensional $K_{\mathfrak{p}}$ vector space with a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action.
2. A arises as a quotient of $J_1(p)$, so $V_{\mathfrak{p}}$ is unramified at $\ell \neq p$.
3. (Eichler-Shimura) The trace of a Frobenius element for ℓ acting on $V_{\mathfrak{p}}$ is a_ℓ and the determinant is $\varepsilon(\ell)\ell$.

Shimura's Construction

Shimura showed there exists an abelian variety $A = A_f/\mathbb{Q}$ associated to f, with the following properties:

1. $\dim(A) = [K : \mathbb{Q}]$, and $K \subseteq \mathrm{End}^0(A_{\overline{\mathbb{Q}}})$, so
$$V_{\mathfrak{p}} := V_p(A) \otimes_{K \otimes \mathbb{Q}_p} K_{\mathfrak{p}}$$
is a 2-dimensional $K_{\mathfrak{p}}$ vector space with a $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$-action.
2. A arises as a quotient of $J_1(p)$, so $V_{\mathfrak{p}}$ is unramified at $\ell \neq p$.
3. (Eichler-Shimura) The trace of a Frobenius element for ℓ acting on $V_{\mathfrak{p}}$ is a_ℓ and the determinant is $\varepsilon(\ell)\ell$.

Write $\rho_f : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}(V_{\mathfrak{p}}) = \mathrm{GL}_2(K_{\mathfrak{p}})$ for this representation.

Irreducibility

For desirable properties of the reduction, we need:

Irreducibility

For desirable properties of the reduction, we need:

Proposition (4.1)

ρ_f is irreducible.

Irreducibility

For desirable properties of the reduction, we need:

Proposition (4.1)

ρ_f is irreducible.

Proof.

If not, then $\rho_f^{ss} = \rho_1 \oplus \rho_2$. A theorem of Serre implies $\rho_i = \chi^{n_i}\varepsilon_i$ where ε_i has finite order ramified only at p.

Irreducibility

For desirable properties of the reduction, we need:

Proposition (4.1)

ρ_f is irreducible.

Proof.

If not, then $\rho_f^{ss} = \rho_1 \oplus \rho_2$. A theorem of Serre implies $\rho_i = \chi^{n_i}\varepsilon_i$ where ε_i has finite order ramified only at p. We get equations for $\ell \neq p$:

$$\ell^{n_1+n_2}\varepsilon_1(\ell)\varepsilon_2(\ell) = \ell\varepsilon(\ell), \text{ and } a_\ell = \varepsilon_1(\ell)\ell^{n_1} + \varepsilon_2(\ell)\ell^{n_2}.$$

Irreducibility

For desirable properties of the reduction, we need:

Proposition (4.1)

ρ_f is irreducible.

Proof.

If not, then $\rho_f^{ss} = \rho_1 \oplus \rho_2$. A theorem of Serre implies $\rho_i = \chi^{n_i}\varepsilon_i$ where ε_i has finite order ramified only at p. We get equations for $\ell \neq p$:

$$\ell^{n_1+n_2}\varepsilon_1(\ell)\varepsilon_2(\ell) = \ell\varepsilon(\ell), \text{ and } a_\ell = \varepsilon_1(\ell)\ell^{n_1} + \varepsilon_2(\ell)\ell^{n_2}.$$

As $n_1 + n_2 = 1$, the second equation gives $|a_\ell| \geq \ell - 1$, contradicting RH $|a_\ell| \leq 2\sqrt{\ell}$ for $\ell \gg 0$. □

Reducing ρ_f

To get good reduction properties, we need a fact about representations over p-adic fields.

Proposition (2.1)

Reducing ρ_f

To get good reduction properties, we need a fact about representations over p-adic fields.

Proposition (2.1)

Let $L/\mathbb{Q}_p$ be finite, V a 2-dimensional L vector space. Suppose a compact group G acts continuously via ρ on V so that V is a simple G-module, but its reductions are reducible.

Reducing ρ_f

To get good reduction properties, we need a fact about representations over p-adic fields.

Proposition (2.1)

Let $L/\mathbb{Q}_p$ be finite, V a 2-dimensional L vector space. Suppose a compact group G acts continuously via ρ on V so that V is a simple G-module, but its reductions are reducible.
Then there is a G-stable lattice $L \subset V$ on whose reduction G acts by upper triangular matrices but not semi-simply.

Reducing ρ_f

To get good reduction properties, we need a fact about representations over p-adic fields.

Proposition (2.1)

Let $L/\mathbb{Q}_p$ be finite, V a 2-dimensional L vector space. Suppose a compact group G acts continuously via ρ on V so that V is a simple G-module, but its reductions are reducible.
Then there is a G-stable lattice $L \subset V$ on whose reduction G acts by upper triangular matrices but not semi-simply.

The proof involves matrix computations and using the p-adic topology.

Finally $\overline{\rho}_f$

From the above, we get

Finally $\overline{\rho}_f$

From the above, we get

Proposition (4.2)

There exists an $\mathcal{O}_\mathfrak{p}$ lattice $L \subset V_\mathfrak{p}$ stable under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ whose residual representation $\overline{\rho}_f$ is an extension of χ^{k-1} by 1 which is not semi-simple.

Finally $\overline{\rho}_f$

From the above, we get

Proposition (4.2)

There exists an $\mathcal{O}_\mathfrak{p}$ lattice $L \subset V_\mathfrak{p}$ stable under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ whose residual representation $\overline{\rho}_f$ is an extension of χ^{k-1} by 1 which is not semi-simple.

Proof.

By Eichler-Shimura and Chebotarev density, the trace and determinant of $\overline{\rho}_f$ agree with $\chi^{k-1} \oplus \mathbf{1}$, so its semi-simplification is isomorphic to this sum. In particular, $\overline{\rho}_f$ is reducible. The claim follows from Prop (2.1). □

Finally $\overline{\rho}_f$

From the above, we get

Proposition (4.2)

There exists an $\mathcal{O}_{\mathfrak{p}}$ lattice $L \subset V_{\mathfrak{p}}$ stable under $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ whose residual representation $\overline{\rho}_f$ is an extension of χ^{k-1} by 1 which is not semi-simple.

Proof.

By Eichler-Shimura and Chebotarev density, the trace and determinant of $\overline{\rho}_f$ agree with $\chi^{k-1} \oplus \mathbf{1}$, so its semi-simplification is isomorphic to this sum. In particular, $\overline{\rho}_f$ is reducible. The claim follows from Prop (2.1). □

This gives (1.3)(i),(ii), & (iii).

Table of Contents

Some Eisenstein Series

- To construct f, we need some Eisenstein series. The following are Hecke eigenforms:

Some Eisenstein Series

- To construct f, we need some Eisenstein series. The following are Hecke eigenforms:
- For $\varepsilon : (\mathbb{Z}/p\mathbb{Z})^\times \to \mu_{p-1}$ a nontrivial even character,

$$G_{2,\varepsilon} := L(-1,\varepsilon) + \sum_{n\geq 1}\sum_{d|n} \varepsilon(d) d q^n.$$

Some Eisenstein Series

- To construct f, we need some Eisenstein series. The following are Hecke eigenforms:
- For $\varepsilon : (\mathbb{Z}/p\mathbb{Z})^\times \to \mu_{p-1}$ a nontrivial even character,

$$G_{2,\varepsilon} := L(-1,\varepsilon) + \sum_{n\geq 1} \sum_{d|n} \varepsilon(d) d q^n.$$

- For ε odd,

$$G_{1,\varepsilon} := L(0,\varepsilon) + \sum_{n\geq 1} \sum_{d|n} \varepsilon(d) q^n.$$

Some Eisenstein Series

- To construct f, we need some Eisenstein series. The following are Hecke eigenforms:
- For $\varepsilon : (\mathbb{Z}/p\mathbb{Z})^\times \to \mu_{p-1}$ a nontrivial even character,

$$G_{2,\varepsilon} := L(-1,\varepsilon) + \sum_{n\geq 1}\sum_{d|n}\varepsilon(d)dq^n.$$

- For ε odd,

$$G_{1,\varepsilon} := L(0,\varepsilon) + \sum_{n\geq 1}\sum_{d|n}\varepsilon(d)q^n.$$

- Fix $\mathfrak{p} \mid p$ in $\mathbb{Q}(\mu_{p-1})$. Let $\omega : (\mathbb{Z}/p\mathbb{Z})^\times \to \mu_{p-1}$ so that $\omega(d) \equiv d \bmod \mathfrak{p}$.

Relation to E_k

- These new Eisenstein series are congruent to the old ones.

Relation to E_k

- These new Eisenstein series are congruent to the old ones.

Lemma (3.1)

Let k be even with $2 \leq k \leq p-3$. Then $G_{2,\omega^{k-2}}$ and $G_{1,\omega^{k-1}}$ have $\mathfrak{p}$-integral expansions in $\mathbb{Q}(\mu_{p-1})$ and are congruent to $E_k \bmod \mathfrak{p}$.

Relation to E_k

- These new Eisenstein series are congruent to the old ones.

Lemma (3.1)

Let k be even with $2 \leq k \leq p-3$. Then $G_{2,\omega^{k-2}}$ and $G_{1,\omega^{k-1}}$ have $\mathfrak{p}$-integral expansions in $\mathbb{Q}(\mu_{p-1})$ and are congruent to E_k mod $\mathfrak{p}$.

- This can be used now to create a modular form g of weight 2, type ω^{k-2} with $\mathfrak{p}$-integral q-expansion with constant term 1. (Theorem 3.3)

Relation to E_k

- These new Eisenstein series are congruent to the old ones.

Lemma (3.1)

Let k be even with $2 \leq k \leq p-3$. Then $G_{2,\omega^{k-2}}$ and $G_{1,\omega^{k-1}}$ have $\mathfrak{p}$-integral expansions in $\mathbb{Q}(\mu_{p-1})$ and are congruent to $E_k \bmod \mathfrak{p}$.

- This can be used now to create a modular form g of weight 2, type ω^{k-2} with $\mathfrak{p}$-integral q-expansion with constant term 1. (Theorem 3.3)
- The proof involves various bounds on cyclotomic field class numbers and special values of L-functions.

Creating f

- Set $\varepsilon = \omega^{k-2}$ and $f' = G_{2,\varepsilon} - cg$ where c is the constant term of $G_{2,\varepsilon}$. By construction, f' is a “semi-cuspform” i.e. it vanishes at the cusp ∞ (but perhaps not the other cusp for $\Gamma_1(p)$).

Creating f

- Set $\varepsilon = \omega^{k-2}$ and $f' = G_{2,\varepsilon} - cg$ where c is the constant term of $G_{2,\varepsilon}$. By construction, f' is a "semi-cuspform" i.e. it vanishes at the cusp ∞ (but perhaps not the other cusp for $\Gamma_1(p)$).
- Since $\mathfrak{p} \mid c$ (since we've assumed $p \mid B_k$...!), we have

$$f' \equiv G_{2,\varepsilon} \equiv E_k \bmod \mathfrak{p}.$$

Creating f

- Set $\varepsilon = \omega^{k-2}$ and $f' = G_{2,\varepsilon} - cg$ where c is the constant term of $G_{2,\varepsilon}$. By construction, f' is a "semi-cuspform" i.e. it vanishes at the cusp ∞ (but perhaps not the other cusp for $\Gamma_1(p)$).
- Since $\mathfrak{p} \mid c$ (since we've assumed $p \mid B_k$...!), we have

$$f' \equiv G_{2,\varepsilon} \equiv E_k \bmod \mathfrak{p}.$$

- Since f' is a cuspform mod $\mathfrak{p}$, a lifting argument of Deligne-Serre gives a semi-cuspform f whose Hecke eigenvalues satisfy

$$a_\ell(f) \equiv 1 + \varepsilon(\ell)\ell \bmod \mathfrak{q}$$

for some $\mathfrak{q} \mid \mathfrak{p}$ in $\mathbb{Q}(\mu_p, \{a_n\})$.

Finishing (3.7)

- Ribet shows f is cuspidal by ruling out the explicit semi-cuspform which is not cuspidal:

$$s_{2,\varepsilon} = \sum_{n \geq 1} \sum_{d|n} \varepsilon(n/d) d q^n.$$

Finishing (3.7)

- Ribet shows f is cuspidal by ruling out the explicit semi-cuspform which is not cuspidal:

$$s_{2,\varepsilon} = \sum_{n \geq 1} \sum_{d|n} \varepsilon(n/d) d q^n.$$

- One checks by comparing eigenvalues that if $f = s_{2,\varepsilon}$, then

$$\varepsilon(\ell) + \ell \equiv 1 + \varepsilon(\ell)\ell \bmod \mathfrak{p}.$$

Finishing (3.7)

- Ribet shows f is cuspidal by ruling out the explicit semi-cuspform which is not cuspidal:

$$s_{2,\varepsilon} = \sum_{n \geq 1} \sum_{d | n} \varepsilon(n/d) d q^n.$$

- One checks by comparing eigenvalues that if $f = s_{2,\varepsilon}$, then

$$\varepsilon(\ell) + \ell \equiv 1 + \varepsilon(\ell)\ell \bmod \mathfrak{p}.$$

- This is not possible since ε is nontrivial.

Finishing (3.7)

- Ribet shows f is cuspidal by ruling out the explicit semi-cuspform which is not cuspidal:

$$s_{2,\varepsilon} = \sum_{n\geq 1} \sum_{d|n} \varepsilon(n/d) d q^n.$$

- One checks by comparing eigenvalues that if $f = s_{2,\varepsilon}$, then

$$\varepsilon(\ell) + \ell \equiv 1 + \varepsilon(\ell)\ell \bmod \mathfrak{p}.$$

- This is not possible since ε is nontrivial.
- Altogether, we get Theorem (3.7): there exists f of weight 2 type ε such that $a_\ell(f) \equiv 1 + \ell^{k-1} \bmod \mathfrak{p}$ for some ideal $\mathfrak{p}$ in K, generated by the a_ℓ.

Table of Contents

Recap

- $C = A/A^p$ for A the class group of $\mathbb{Q}(\mu_p)$. We want to show $p \mid B_k$ implies $C(\chi^{1-k}) \neq 0$. By CFT, we need to create a special Galois representation $\overline{\rho}$ to build a special unramified extension of $\mathbb{Q}(\mu_p)$.

Recap

- $C = A/A^p$ for A the class group of $\mathbb{Q}(\mu_p)$. We want to show $p \mid B_k$ implies $C(\chi^{1-k}) \neq 0$. By CFT, we need to create a special Galois representation $\overline{\rho}$ to build a special unramified extension of $\mathbb{Q}(\mu_p)$.
- The assumption $p \mid B_k$ suggests that the Eisenstein series E_k will be cuspidal mod p. With some work, we can show the existence of a nice cuspform $f \equiv E_k$ modulo a certain prime ideal in a bigger field.

Recap

- $C = A/A^p$ for A the class group of $\mathbb{Q}(\mu_p)$. We want to show $p \mid B_k$ implies $C(\chi^{1-k}) \neq 0$. By CFT, we need to create a special Galois representation $\overline{\rho}$ to build a special unramified extension of $\mathbb{Q}(\mu_p)$.
- The assumption $p \mid B_k$ suggests that the Eisenstein series E_k will be cuspidal mod p. With some work, we can show the existence of a nice cuspform $f \equiv E_k$ modulo a certain prime ideal in a bigger field.
- Using the Tate module of a modular Jacobian, we can attach a representation ρ_f of the Galois group to f whose values on Frobenius elements relate to the Hecke eigenvalues of f.

Recap (2)

- Taking a particular reduction of ρ_f yields the desired $\overline{\rho}$ in (1.3): the congruence $f \equiv E_k$ means it will be an extension of χ^{k-1} by $\mathbf{1}$ but not diagonalizable, and have the other properties we wanted.

Recap (2)

- Taking a particular reduction of ρ_f yields the desired $\overline{\rho}$ in (1.3): the congruence $f \equiv E_k$ means it will be an extension of χ^{k-1} by $\mathbf{1}$ but not diagonalizable, and have the other properties we wanted.
- Then $\ker \overline{\rho}$ creates the unramified abelian extension of $\mathbb{Q}(\mu_p)$ corresponding to $C(\chi^{1-k}) \neq 0$.

Bonus!

- What about (1.3)(iv), namely the condition that $\overline{\rho}|_D$ be diagonalizable for D a decomposition group for p?

Bonus!

- What about (1.3)(iv), namely the condition that $\overline{\rho}|_D$ be diagonalizable for D a decomposition group for p?
- Let M be the space for $\overline{\rho}$. To show p does not divide the size of the image of D under $\overline{\rho}$, restrict to the subgroup $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_p)^+)$ since $p \nmid [\mathbb{Q}(\mu_p)^+ : \mathbb{Q}]$. Let F be the completion of $\mathbb{Q}(\mu_p)^+$ with respect to the prime above p.

Bonus!

- What about (1.3)(iv), namely the condition that $\overline{\rho}|_D$ be diagonalizable for D a decomposition group for p?
- Let M be the space for $\overline{\rho}$. To show p does not divide the size of the image of D under $\overline{\rho}$, restrict to the subgroup $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_p)^+)$ since $p \nmid [\mathbb{Q}(\mu_p)^+ : \mathbb{Q}]$. Let F be the completion of $\mathbb{Q}(\mu_p)^+$ with respect to the prime above p.
- One shows M is the "Galois module of a finite flat group scheme $\mathcal{M}$ of type $(p, \ldots, p)$ over $\mathcal{O}_F$."

Bonus!

- What about (1.3)(iv), namely the condition that $\overline{\rho}|_D$ be diagonalizable for D a decomposition group for p?
- Let M be the space for $\overline{\rho}$. To show p does not divide the size of the image of D under $\overline{\rho}$, restrict to the subgroup $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}(\mu_p)^+)$ since $p \nmid [\mathbb{Q}(\mu_p)^+ : \mathbb{Q}]$. Let F be the completion of $\mathbb{Q}(\mu_p)^+$ with respect to the prime above p.
- One shows M is the "Galois module of a finite flat group scheme $\mathcal{M}$ of type $(p, \ldots, p)$ over $\mathcal{O}_F$."
- Using an argument with the connected-étale sequence for $\mathcal{M}$, one creates two distinct lines in M preserved by D. Any element of order p would preserve a *unique* line however.