Automorphic forms seminar

Tuesday, May 10, 2022 2:43 PM

A modular construction of unramified p-extensions of $\mathbb{Q}(N^{1/p})$

p: odd prime, ζ_p: primitive p-th root of 1

$$\begin{tikzcd} \chi_p : G_{\mathbb{Q}} = \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \arrow[r] \arrow[dr, "\omega"'] & \mathbb{Z}_p^\times \arrow[d, "\text{mod } p"] \\ & \mathbb{F}_p^\times \end{tikzcd}$$

p-adic cyc. char

I. Ribet and $\mathbb{Q}(\zeta_p)$

$2 \le k \le p-3$ even

Q: When does $\exists F/\mathbb{Q}(\zeta_p)$ Gal., deg. p, unram. s.t.
- $F/\mathbb{Q}$ is Gal.
- $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$ act on $\mathrm{Gal}(F/\mathbb{Q}(\zeta_p))$ by ω^{1-k}?

Th'm: (Ribet '76) Such an ext'n exists iff $p \mid \underbrace{B_k}_{k\text{th Bernoulli number}}$.

Sps. $F/\mathbb{Q}(\zeta_p)$ exists.

$$\bar\rho : G_{\mathbb{Q}} \to \mathrm{Gal}(F/\mathbb{Q}) \cong \underbrace{\mathrm{Gal}(F/\mathbb{Q}(\zeta_p))}_{\cong\, \mathbb{Z}/p\mathbb{Z}} \rtimes \underbrace{\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})}_{\cong\, (\mathbb{Z}/p\mathbb{Z})^\times} \hookrightarrow GL_2(\mathbb{F}_p)$$

$$(1,1) \longmapsto \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$$

$$(0,g) \longmapsto \begin{pmatrix} 1 & 0 \\ 0 & g^{k-1} \end{pmatrix}$$

Then $F = \overline{\mathbb{Q}}^{\ker \bar\rho}$.

Th'm: (Ribet, v2) If $p \mid B_k$, then $\exists \bar\rho : G_{\mathbb{Q}} \to GL_2(\mathbb{F}_p)$ s.t.

✓(i) $\bar\rho$ is unram. outside p

✓(ii) $\bar\rho$ is reducible, nonsemisimple: $\bar\rho = \begin{pmatrix} 1 & \overset{\neq 0}{*} \\ 0 & \omega^{k-1} \end{pmatrix}$

* (iii) $\bar\rho|_{D_p}$ is semisimple.

So $\overline{\mathbb{Q}}^{\ker\bar\rho}/\mathbb{Q}(\zeta_p)$ is unram, nontrivial, $(p, \dots, p)$-ext'n with $\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})$-action given by ω^{1-k}.

How to produce $\bar{\rho}$?

<u>Key Lemma</u>: (Ribet) $K/\mathbb{Q}_p$ fin., $\mathcal{O} \subset K$ ring of ints, $\varpi \in \mathcal{O}$ unif. If $\rho : G_{\mathbb{Q}} \to GL_2(\mathcal{O})$ is irred. over K and $\bar{\rho} := \rho \bmod \varpi$ is reducible, say $\bar{\rho}^{ss} \cong \psi_1 \oplus \psi_2$, then $\exists x \in GL_2(K)$ s.t. $r := x\rho x^{-1} : G_{\mathbb{Q}} \to GL_2(\mathcal{O})$ and $\bar{r} = \begin{pmatrix} \psi_1 & * \neq 0 \\ 0 & \psi_2 \end{pmatrix}$.

→ Cusp forms give irred. Gal. reps. in char. 0

→ Eisenstein series have correct Gal. rep. mod ϖ:

$$E_k(z) = \frac{-B_k}{2k} + \sum_{n \geq 1} \Big(\sum_{0 < d \mid n} d^{k-1} \Big) q^n \qquad (q = e^{2\pi i z})$$

has Gal. rep. $\mathbb{1} \oplus \chi_p^{k-1}$.

If $k \geq 4$, then $E_k \in M_k(SL_2(\mathbb{Z}))$.

$\therefore$ Want Eisenstein-cuspidal congruence: $f \in S_k(SL_2(\mathbb{Z}))$ s.t.

$$f \equiv E_k \pmod{\mathfrak{p}} \qquad \mathfrak{p} \mid p.$$

<u>Rmk</u>: If f exists, then

$$0 = a_0(f) \equiv a_0(E_k) = -\frac{B_k}{2k} \pmod{\mathfrak{p}}.$$

So $p \mid B_k$.

<u>Th'm</u>: ("Ribet") If $p \mid B_k$, then $\exists f \in S_k(SL_2(\mathbb{Z}))$ s.t. $f \equiv E_k \pmod{\mathfrak{p}}$ some $\mathfrak{p} \mid p$.

Use $\rho_{f,\mathfrak{p}}$ in Key Lemma to get $\bar{\rho} : G_{\mathbb{Q}} \to GL_2(\mathbb{F}_p)$ unram. outside p s.t. $\bar{\rho} = \begin{pmatrix} 1 & * \neq 0 \\ 0 & \omega^{1-k} \end{pmatrix}$.

Checking $\bar{\rho}|_{D_p}$ is semisimple is nontrivial, but can be done.

II. L.-Wake and $\mathbb{Q}(N^{1/p})$

N prime, $p \geq 5$

<u>Q</u>: When $\exists\, F/\mathbb{Q}(N^{1/p})$ Gal., deg. p, unram.?

i.e. When does $p \mid \# \mathrm{Cl}(\mathbb{Q}(N^{1/p}))$?

<u>Observation</u>: If $N \equiv 1 \ (p)$, then

$$\begin{array}{c} \mathbb{Q}(\zeta_N) \\ | \\ \exists\, K \\ |\,p \\ \mathbb{Q} \end{array}$$

Easy to check $F := K(N^{1/p})/\mathbb{Q}(N^{1/p})$ is unram. at N,
so $p \mid \# \mathrm{Cl}(\mathbb{Q}(N^{1/p}))$.

<u>Th'm</u>: (Iimura, Calegari, L.-Wake)
alg. no. th'y, Gal. cohom., modular forms

$$N \equiv -1 \ (p) \implies p \mid \# \mathrm{Cl}(\mathbb{Q}(N^{1/p})).$$

Sps. $F/\mathbb{Q}(N^{1/p})$ exists. (Gal, deg p, unram.)
$\tilde{F} :=$ Galois closure of F over $\mathbb{Q}$.

$$\bar{\rho} : G_{\mathbb{Q}} \to \mathrm{Gal}(\tilde{F}/\mathbb{Q}) \to \mathrm{Gal}(\mathbb{Q}(\zeta_p, N^{1/p})/\mathbb{Q}) \cong \underbrace{\mathrm{Gal}(\mathbb{Q}(\zeta_p, N^{1/p})/\mathbb{Q}(N^{1/p}))}_{\cong\, \mathbb{Z}/p\mathbb{Z}} \rtimes \underbrace{\mathrm{Gal}(\mathbb{Q}(\zeta_p)/\mathbb{Q})}_{\cong\, (\mathbb{Z}/p\mathbb{Z})^\times} \hookrightarrow G$$

$$\bar{\rho} = \begin{pmatrix} \omega & * \\ 0 & 1 \end{pmatrix}$$

Want $k=2$, but $E_2 \notin M_2(SL_2(\mathbb{Z}))$.

$$E_{2,N}(z) := E_2(z) - N E_2(Nz) \in M_2(\Gamma_0(N))$$
$$= \underline{\frac{N-1}{24}} + \sum_{n \geq 1} \Big(\sum_{\substack{0<d \mid n \\ N \nmid d}} d \Big) q^n.$$

<u>Th'm</u>: (Mazur) Sps. $p \geq 5$.
$\exists f \in S_2(\Gamma_0(N))$ s.t. $f \equiv E_{2,N} \pmod{\mathfrak{p}} \iff N \equiv 1 \ (\mathfrak{p})$.

$\underline{E(z)} := N E_{2,N}(z) - N E_{2,N}(Nz) \in M_2(\Gamma_0(N^2))$

$T_\ell E = (\ell+1) E \quad \forall \ell \neq N$ prime, $\quad U_N E = 0.$

Th'm: (L.-Wake) If $N \equiv -1 \ (p)$, then $\exists f \in \underline{S_2(\Gamma_0(N^2))}$ and $\wp | p$ s.t. $f \equiv \underline{E} \pmod{\wp}$.

Fix such an f.

$K = \mathbb{Q}_p(a_n(f) : n \geq 1)$

$\cup$

$\mathcal{O}$: ring of ints

$\cup$

ϖ : uniformizer

(*) Assume $f \not\equiv E \pmod{\varpi^2}$.

Ribet Key Lemma $\rightsquigarrow \rho = \rho_f : G_\mathbb{Q} \to GL_2(\mathcal{O})$

→ unram. outside Np

→ $\bar\rho = \begin{pmatrix} \omega & \bar b \\ 0 & 1 \end{pmatrix}$ $\qquad \bar b \in H^1(\mathbb{Q}^{Np}, \mathbb{F}_p(1)) = \langle \kappa_N, \kappa_p \rangle$

$\kappa_N(\sigma) := \dfrac{\sigma(N^{1/p})}{N^{1/p}}$

$p \nmid N^2 =$ level of f $\implies \bar b = \kappa_N$

$\implies \mathbb{Q}(N^{1/p})$ is the splitting field of $\bar b$.

$r := \rho \bmod \varpi^2 : G_\mathbb{Q} \longrightarrow GL_2(\mathcal{O}/\varpi^2)$

$r|_{G_{\mathbb{Q}(N^{1/p})}} = \begin{pmatrix} \chi_p(1+a\varpi) & b\varpi \\ c\varpi & 1-a\varpi \end{pmatrix}$

$\chi := 1 + a\varpi$ is a character.

→ unram. outside Np

→ $\chi^p = 1$

$F := \overline{\mathbb{Q}(N^{1/p})}^{\ker \chi}$ is our candidate.

We show:

1) $f \not\equiv E \pmod{\varpi^2} \implies \chi \neq 1$.

2) χ unram. at N: $N \not\equiv 1\ (p) \Rightarrow \nexists$ p-power order chars. of $I_N \leq G_{\mathbb{Q}_N(N^{1/p})}$.

3) χ unram at p: follows from f ord. at p, so

$$\rho_f|_{D_f} \sim \begin{pmatrix} \chi_p & * \\ 0 & 1 \end{pmatrix}.$$

Advantages of a modular proof: $\underline{N \equiv -1\ (p)}$ $\underline{f \not\equiv E\ (\varpi^2)}$.

<u>Th'm</u>: (L.-Wake) Sps. $\# Cl(\mathbb{Q}(N^{1/p})) = p$.
Let λ be a prime of $\mathbb{Q}(N^{1/p})$ lying over $\ell \nmid Np$.

1) Sps. $\ell \not\equiv 1\ (p)$. If $f(\lambda|\ell) = 1$, then TFAE:
   a) λ is principal
   b) λ splits in the Hilbert class field of $\mathbb{Q}(N^{1/p})$
   c) ℓ is a norm from $\mathbb{Q}(N^{1/p})$
   d) $a_\ell(f) \equiv \ell + 1 \pmod{\varpi^2}$.

2) Sps. $\ell \equiv 1\ (p)$. If $a_\ell(f) \not\equiv 2 \pmod{\varpi^2}$, then ℓ is inert in $\mathbb{Q}(N^{1/p})$.

<u>Ex</u>: $N = 19$, $p = 5$

You can compute these coefficients! (Sage, LMFDB)

$\beta := \frac{1+\sqrt{5}}{2}$, $\beta \equiv 3 \bmod \sqrt{5}$, Note: $a_\ell \equiv \ell + 1 \bmod \sqrt{5}$

ℓ	a_ℓ	ℓ	a_ℓ	ℓ	a_ℓ
2	β	53	$5-7\beta$	127	$9-2\beta$
3	$2-\beta$	59	$-11+7\beta$	131	$7+5\beta$
5	2β	61	$-7-2\beta$	137	$1+4\beta$
7	3	67	-7	139	$-3+11\beta$
11	$-\beta$	71	$-1-4\beta$	149	$-10+5\beta$
13	-1	73	$7-6\beta$	151	$-13-5\beta$
17	$4-2\beta$	79	$-6+12\beta$	157	$-13-3\beta$
19	0	83	$2+4\beta$	163	$5-2\beta$
23	$7-\beta$	89	$-11+2\beta$	167	$17+2\beta$
29	$-2-\beta$	97	$9+3\beta$	173	$6-4\beta$
31	$-4-3\beta$	101	$7-10\beta$	179	$9+2\beta$
37	$4+3\beta$	103	$3+7\beta$	181	12
41	-3	107	$-3+12\beta$	191	$11+2\beta$
43	$5+3\beta$	109	$-1+6\beta$	193	$18-8\beta$
47	3	113	$10-2\beta$	197	3

You can compute these coefficients! (Sage, LMFDB)

$\beta := \frac{1+\sqrt{5}}{2}$, $a_\ell \not\equiv \ell + 1 \bmod 5$, $a_\ell \equiv \ell + 1 \bmod 5$

ℓ	a_ℓ	ℓ	a_ℓ	ℓ	a_ℓ
2	β	53	$5-7\beta$	127	$9-2\beta$
3	$2-\beta$	59	$-11+7\beta$	131	$7+5\beta$
5	2β	61	$-7-2\beta$	137	$1+4\beta$
7	3	67	-7	139	$-3+11\beta$
11	$-\beta$	71	$-1-4\beta$	149	$-10+5\beta$
13	-1	73	$7-6\beta$	151	$-13-5\beta$
17	$4-2\beta$	79	$-6+12\beta$	157	$-13-3\beta$
19	0	83	$2+4\beta$	163	$5-2\beta$
23	$7-\beta$	89	$-11+2\beta$	167	$17+2\beta$
29	$-2-\beta$	97	$9+3\beta$	173	$6-4\beta$
31	$-4-3\beta$	101	$7-10\beta$	179	$9+2\beta$
37	$4+3\beta$	103	$3+7\beta$	181	12
41	-3	107	$-3+12\beta$	191	$11+2\beta$
43	$5+3\beta$	109	$-1+6\beta$	193	$18-8\beta$
47	3	113	$10-2\beta$	197	3

You can compute these coefficients! (Sage, LMFDB)

$\beta := \frac{1+\sqrt{5}}{2}$, $a_\ell \not\equiv \ell + 1 \bmod 5$, $a_\ell \equiv \ell + 1 \bmod 5$, $\ell \equiv 1 \bmod 5$

ℓ	a_ℓ	ℓ	a_ℓ	ℓ	a_ℓ
2	β	53	$5-7\beta$	127	$9-2\beta$
3	$2-\beta$	59	$-11+7\beta$	131	$7+5\beta$
5	2β	61	$-7-2\beta$	137	$1+4\beta$
7	3	67	-7	139	$-3+11\beta$
11	$-\beta$	71	$-1-4\beta$	149	$-10+5\beta$
13	-1	73	$7-6\beta$	151	$-13-5\beta$
17	$4-2\beta$	79	$-6+12\beta$	157	$-13-3\beta$
19	0	83	$2+4\beta$	163	$5-2\beta$
23	$7-\beta$	89	$-11+2\beta$	167	$17+2\beta$
29	$-2-\beta$	97	$9+3\beta$	173	$6-4\beta$
31	$-4-3\beta$	101	$7-10\beta$	179	$9+2\beta$
37	$4+3\beta$	103	$3+7\beta$	181	12
41	-3	107	$-3+12\beta$	191	$11+2\beta$
43	$5+3\beta$	109	$-1+6\beta$	193	$18-8\beta$
47	3	113	$10-2\beta$	197	3

You can compute these coefficients! (Sage, LMFDB)

(ℓ, a_ℓ) or (ℓ, a_ℓ) $\implies$ $\exists$ principal prime of $\mathbb{Q}(19^{1/5})$ over ℓ

ℓ	a_ℓ	ℓ	a_ℓ	ℓ	a_ℓ
2	β	53	$5-7\beta$	127	$9-2\beta$
3	$2-\beta$	59	$-11+7\beta$	131	$7+5\beta$
5	2β	61	$-7-2\beta$	137	$1+4\beta$
7	3	67	-7	139	$-3+11\beta$
11	$-\beta$	71	$-1-4\beta$	149	$-10+5\beta$
13	-1	73	$7-6\beta$	151	$-13-5\beta$
17	$4-2\beta$	79	$-6+12\beta$	157	$-13-3\beta$
19	0	83	$2+4\beta$	163	$5-2\beta$
23	$7-\beta$	89	$-11+2\beta$	167	$17+2\beta$
29	$-2-\beta$	97	$9+3\beta$	173	$6-4\beta$
31	$-4-3\beta$	101	$7-10\beta$	179	$9+2\beta$
37	$4+3\beta$	103	$3+7\beta$	181	12
41	-3	107	$-3+12\beta$	191	$11+2\beta$
43	$5+3\beta$	109	$-1+6\beta$	193	$18-8\beta$
47	3	113	$10-2\beta$	197	3