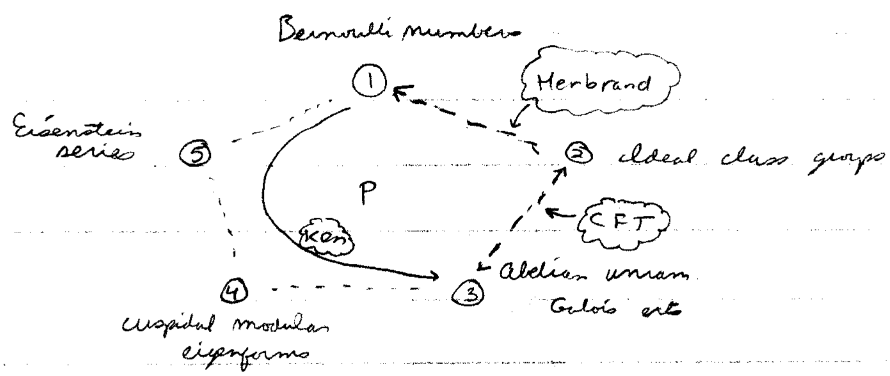
6-[illegible]-00
Barry Mazur

Construction of abelian extensions following Ribet:



$p = 691$

$p =$ any prime

1 Bernoulli numbers

$$\frac{B_{2k}}{4k} =$$

$$\frac{B_2}{4} = \frac{1}{24},\ \frac{1}{240},\ \frac{1}{504},\ \frac{1}{480},\ \frac{1}{264},\ \frac{691}{65520} = \frac{B_{12}}{24}$$

$$\frac{B_{12}}{24} \equiv 0 \ (\mathrm{mod}\ 691)$$

2 $K = \mathbb{Q}(e^{2\pi i/691})$ $\qquad \mathrm{Gal}(K/\mathbb{Q}) \simeq \mathbb{F}_{691}^{\times}$

$$\gamma \in \mathrm{Gal}(K/\mathbb{Q})$$

$$\gamma(e^{2\pi i/691}) = e^{2\pi i \gamma/691}$$

(ideal class group)

There is a cyclic quotient of I.C.G. X of order 691 that is stable under $\mathbb{F}_{691}^{\times}$.

$$\gamma(x) = \gamma^{1-12}(x) = \gamma^{-11}x.$$

3 $K = \mathbb{Q}(e^{2\pi i/691}) / \mathbb{Q}$

We want L/K that is cyclic of degree 691.:

$$\text{Galois}\left[\begin{array}{l} L \\ {\scriptstyle 691}\,|\ y \\ K \\ {\scriptstyle 690}\,|\ \mathbb{F}_{691}^{\times} \ni \gamma \\ \mathbb{Q} \end{array}\right.$$

L/K everywhere unramified.

$$\gamma y \gamma^{-1} = \gamma^{-11} y$$

④ $\Delta(q) = q \prod_{n=1}^{\infty} (1-q^n)^{24}$ $\qquad q = e^{2\pi i z}, z \in \mathfrak{H}$.

$$= 0 + \sum_{n=1}^{\infty} \tau(n) q^n$$

$n \longmapsto \tau(n)$

$\boxed{\ell \longmapsto \tau(\ell)}$ prime ℓ, these determine all the values of $\tau(n)$

$\tau(n) \equiv \sum_{d|n} d^{11} \pmod{691}$, i.e., $\tau(\ell) \equiv 1 + \ell^{11} \pmod{691}$.

This is a wt. 12 level 1 modular form.

⑤ $E_{12} = \frac{B_{12}}{24} + \sum_{n=1}^{\infty} \left(\sum_{d|n} d^{11} \right) q^n$. $\qquad$ wt 12

$\quad\ \ \equiv \qquad\qquad\quad \equiv \pmod{691}$

$\quad\ \ 0 \qquad\qquad\quad \tau(n)$

E_{12} looks cuspidal mod 691

$E_{12} \equiv \Delta \pmod{691}$.

Now let p be an arbitrary prime. Let $2 < 2k < p-1$.

Theorem (H-R): These are equivalent:

① $B_{2k}/4k \equiv 0 \pmod p$.

⑤ $E_{2k} = -B_{2k}/4k + \sum_{n=1}^{\infty} \left(\sum_{d|n} d^{2k-1} \right) q^n$ looks cuspidal modulo p.

④ For every weight $w \geq 2$ there are

ⓐ Common field

$$\begin{array}{ccc} \mathbb{C} & & \overline{\mathbb{Q}}_p \\ & \diagdown \; \diagup & \\ & F_w \ni t_w(n) & \end{array}$$

ⓑ Power series

$$\Phi_w = 0 + \sum t_w(n) q^n$$

In terms of $\mathbb{C}$, Φ_w is a cuspidal modular eigenform of weight w on $\Gamma_1(p)$.

In terms of $\overline{\mathbb{Q}}_p$, $t_w(n) \equiv (\bmod\ \varpi) \equiv \sum_{d|n} d^{2k-1} \pmod p$.

<u>Ken:</u> $\boxed{w=2}$

$p = 691$

$\Phi_{12} = $ "Δ"

$\Phi_2 \sim F_2$

$$\begin{array}{c} F_2 \\ \Big| \, 2508 \\ \mathbb{Q} \end{array}$$

③ There is a Galois extension

$$\begin{array}{l} L \\ p \Big| \; Y \\ K = \mathbb{Q}(e^{2\pi i/p}) \\ \Big| \; \mathbb{F}_p^\times \ni \gamma \\ \mathbb{Q} \end{array}$$

$\gamma(y)\gamma^{-1} = \gamma^{1-2k} y$

On the LHS, we consider γ lifted to $Gal(L/\mathbb{Q})$, the RHS it is just in $Gal(K/\mathbb{Q})$.

L/K everywhere unramified.

How do we get from ④ to ③?

Consider (Δ, p).

$$\begin{array}{ll} & \overline{\mathbb{Q}} \\ G_{\mathbb{Q}} & \Big| \\ & \mathbb{Q}(\text{unram outside } p) \\ & \Big| \qquad\qquad G_{\mathbb{Q},\{p\}} \\ & \mathbb{Q} \end{array}$$

Deligne gives $\rho_{\Delta,p} : G_{\mathbb{Q},p} \to GL_2(\mathbb{Q}_p)$ irred. cont.

$p \neq \ell$ $\quad \{\mathrm{Frob}_\ell\} \subset G_{\mathbb{Q},p}$

$\mathrm{Tr}(\rho_{\Delta p}(\mathrm{Frob}_\ell)) = \tau(\ell) \quad \forall \ell \neq p.$

$(\Delta, 691)$:

$$\begin{tikzcd} G_{\mathbb{Q}p} \arrow[r] \arrow[dr, dashed] & GL_2(\mathbb{Q}_p) \\ & GL_2(\mathbb{Z}_p) \arrow[u, phantom, "\cup"] \arrow[d] \\ & GL_2(\mathbb{F}_p) \end{tikzcd}$$

$\tau(\ell) \equiv 1 + \ell^{11} \pmod{691} \quad \Rightarrow$

$\rho_{\Delta,691}^{ss} = \mathbb{1} \oplus \omega^{11}$ What are possible forms for $\rho_{\Delta,691} \pmod p$?

$\begin{pmatrix} \omega^{11} & * \\ 0 & \mathbb{1} \end{pmatrix}$ $\quad \boxed{\begin{pmatrix} \mathbb{1} & * \\ 0 & \omega^{11} \end{pmatrix}}$ Can show $* \neq 0$.

L ← splitting field

$691 \mid$

$K = \mathbb{Q}(e^{2\pi i/691})$

$\mid$

$\mathbb{Q}$

"The wrench": Appropriate L will be unramified.

The wrench:

Toy: $E = X_1(11)/\mathbb{Q}$ elliptic curve

$p = 5.$

$E[5]$ ← these both occur as subrep and qt when we restrict to D_5.

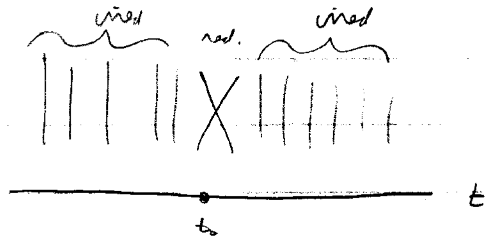
$G_{\mathbb{Q}}$: $0 \to \mathbb{Z}/5\mathbb{Z} \to E[5] \to \mu_5 \to 0.$

$\cup$

D_5: $0 \to \mu_5 \to E[5] \to \mathbb{Z}/5\mathbb{Z} \to 0$

Thus, the rep is semi simple!

Modern:



$\rho_t : G_{\mathbb{Q}} \to GL_2(\mathbb{Q}_p)$.

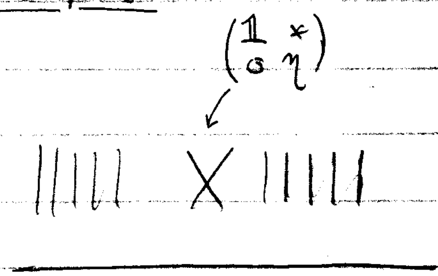
ordinary (i.e. $\rho_t|_{D_p}$ has an unram deg 1 subrep for each t)

straight lines mean irred,
other means red.

$\rho_{t_0} = \begin{pmatrix} \chi_1 & * \\ 0 & \chi_2 \end{pmatrix}$ globally

There are basically two possibilities, $* \neq 0$ and then χ_1 unram where $* = 0$, or χ_2 unram.

The template:



$\longrightarrow$ Cohomology of η (good.)

$0 \to \eta \to \mathcal{E} \to \mathbb{1} \to 0$

η	char. mod p	Ken Ribet
	char p-adic	Main Conj. tot. real fields
	Hecke char/quad imag field	Bellaïche
	GL_2-rep	Skinner-Urban, Bellaïche-Chenevier
	$\vdots$	