

Polynomials equations modulo p:

1) Quadratic equation: $f(x) = x^2 - x - 1$.

$$n(p) = |\{x \pmod{p} : f(x) \equiv 0 \pmod{p}\}| = 1 + \left(\frac{5}{p}\right) = 1 + \left(\frac{p}{5}\right)$$

$$= \begin{cases} 0 & p \equiv 2, 3 \pmod{5} \\ 1 & p = 5 \\ 2 & p \equiv 1, 4 \pmod{5} \end{cases}$$

Roots: $\frac{1 \pm \sqrt{5}}{2}$.

Fix $j \in \{0, 2\}$. $\delta(\{p : n(p) = j\}) = 1/2$
 ↑ density.

2) Cubic equation: $f(x) = x^3 - x - 1$.

disc(f) = -23

Note: $f(x) \equiv (x-3)(x-10)^2 \pmod{23}$

$\Rightarrow n(23) = 2$.

$\forall p \neq 23, n(p) \in \{0, 1, 3\}$.

Questions: Fix $j \in \{0, 1, 3\}$.

1) Formula/generating function for $n(p)$? ($1 + a(p)$?)

Answer arises from modular forms.

2) Describe $\{p : n(p) = j\}$.
 3) Compute $\delta(\{p : n(p) = j\})$.
 algebraic number theory.

Def: $f_{23}(q) = q \prod_{m=1}^{\infty} (1 - q^m)(1 - q^{23m}), |q| < 1$.

$\{a(n)\}$ $f_{23}(q) = \sum_{n=1}^{\infty} a(n)q^n = q - q^2 - q^3 + q^6 + \dots$

Theorem: $\forall p, \quad n(p) = 1 + a(p).$

Modular forms:

$$H = \{ z \in \mathbb{C} : \text{Im}(z) > 0 \}$$

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) : N|c \right\}.$$

$f: H \rightarrow \mathbb{C}$ is a modular form of weight $k \in \mathbb{Z}$ on $\Gamma_0(N)$ with Nebentypus χ (Dirichlet character mod N) if

1) $\forall \gamma \in \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$

$$f(\gamma z) = \chi(d)(cz+d)^k f(z).$$

2) f is holomorphic on H and at cusps.

$$q = e^{2\pi iz} \quad f(z) = \sum_{n=0}^{\infty} a_f(n) q^n \in M_k(\Gamma_0(N), \chi).$$

$$M_k(\Gamma_0(N), \chi) \supseteq S_k(\Gamma_0(N), \chi) \quad \text{cusp forms.}$$

Def: $\eta(z) = q^{1/24} \prod_{m=1}^{\infty} (1 - q^m);$

$$f_{23}(z) = \eta(z) \eta(23z) = \sum_{n=1}^{\infty} a(n) q^n = q + \dots$$

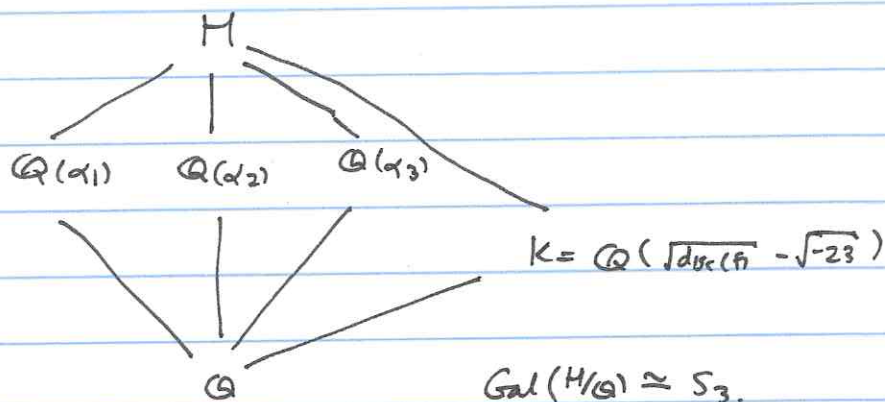
Fact: $f_{23}(z) \in S_1(\Gamma_0(23), \left(\begin{smallmatrix} 1 & \\ & 23 \end{smallmatrix} \right))$
 $\text{dim}_{\mathbb{C}} = 1$

$\Rightarrow f_{23}$ is an eigenvector for all Hecke operators

$$\Rightarrow \forall m, n, \gcd(m, n) = 1, a(mn) = a(m)a(n).$$

Algebraic Number Theory:

$$f(x) = x^3 - x - 1 \quad \text{Roots} = \{\alpha_1, \alpha_2, \alpha_3\}, \quad H = \text{splitting field}$$



$$K \leftrightarrow \mathbb{Z}/3\mathbb{Z}$$

Basic idea:

Thm: (efg): F/\mathbb{Q} , # field, $p \in \text{TP}_{\mathbb{Q}} = \text{primes of } \mathbb{Q}$.

$$\bullet (p) = p\mathcal{O}_F = \underbrace{\mathfrak{p}_1^{e_1} \dots \mathfrak{p}_g^{e_g}}_{\text{unique}}$$

$$\bullet \forall i, | \mathcal{O}_F / \mathfrak{p}_i | = p^{f_i}$$

$$\Rightarrow \sum_{i=1}^g e_i f_i = [F:\mathbb{Q}]$$

F/\mathbb{Q} Galois $\Rightarrow \forall i, e_i = e, f_i = f$

$$\bullet (p) = (\mathfrak{p}_1 \dots \mathfrak{p}_g)^e$$

$$\bullet efg = [F:\mathbb{Q}]$$

Thm (Kummer): Θ : alg. number with minimal poly. $f_{\Theta}(x)$

$F = \mathbb{Q}[\Theta]$. Let $p \in \mathbb{P}_{\mathbb{Q}}$, $p \nmid [F:\mathbb{Q}]$.

$$f_{\Theta}(x) \equiv h_1(x)^{e_1} \cdots h_g(x)^{e_g} \pmod{p}$$

with h_i irred. in $\mathbb{F}_p[x]$. We have

1) $\mathfrak{p}_i = (p, h_i(\Theta)) \triangleq \mathcal{O}_F$ prime

2) $(p) = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_g^{e_g}$.

3) $\deg h_i = f_i$.

Frobenius: associate to $p \in \mathbb{P}_{\mathbb{Q}}$:

F/\mathbb{Q} Galois number field, $(p) = \mathfrak{p}_1 \cdots \mathfrak{p}_g$.

$$\text{Gal}(\mathcal{O}_F/\mathfrak{p}_i / \mathbb{Z}/p\mathbb{Z}) = \langle \sigma_p : x \mapsto x^p \rangle$$

$$\cong \mathbb{Z}/f\mathbb{Z}$$

$$\cong D_{\mathfrak{p}_i} \subseteq \text{Gal}(F/\mathbb{Q})$$



decomposition
group

Then $\text{Frob}_{\mathfrak{p}_i}$ is the element of $D_{\mathfrak{p}_i}$ corresponding to σ_p .

• $\text{Frob}_p = \{ \text{Frob}_{\mathfrak{p}_i} \}$ ← conjugacy class in $\text{Gal}(F/\mathbb{Q})$.

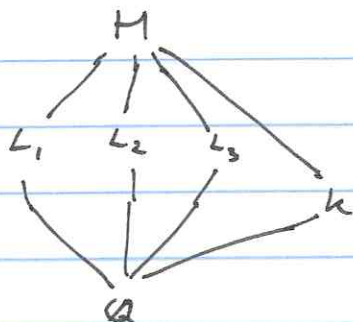
• $\# f = \text{ord}(\text{Frob}_p)$ in $\text{Gal}(F/\mathbb{Q})$

Thm (Chebotarev): Let $\sigma \in \text{Gal}(F/\mathbb{Q})$, $\text{Cl}(\sigma) =$ conjugacy class

of σ in $\text{Gal}(F/\mathbb{Q})$. We have

$$\delta(\{ p \in \mathbb{P}_{\mathbb{Q}} : \text{Frob}_p = \text{Cl}(\sigma) \}) = \frac{|\text{Cl}(\sigma)|}{|\text{Gal}(F/\mathbb{Q})|}$$

$$f(x) = x^3 - x - 1 \quad n(p) = \# \text{ sols (mod } p)$$



$n(p)$	\mathcal{O}_{L_i}		\mathcal{O}_K	\mathcal{O}_M	$\# \text{ (Frob in } G_M)$
0	(p)	$(f=3)$	$\mathcal{O}_1, \mathcal{O}_2$	R, R_2	3
1	$\mathfrak{p}_1, \mathfrak{p}_2$	$(f_1=1, f_2=2)$	(p)	R, R_2, R_3	2
3	$\mathfrak{p}_1, \mathfrak{p}_2, \mathfrak{p}_3$	$(f_i=1)$	$\mathcal{O}_1, \mathcal{O}_2$	R, R_2, \dots, R_6	1

} efg

$$\frac{2}{3} \quad (2 \text{ 3-cycles})$$

$$\frac{1}{2} \quad (3 \text{ 2-cycles})$$

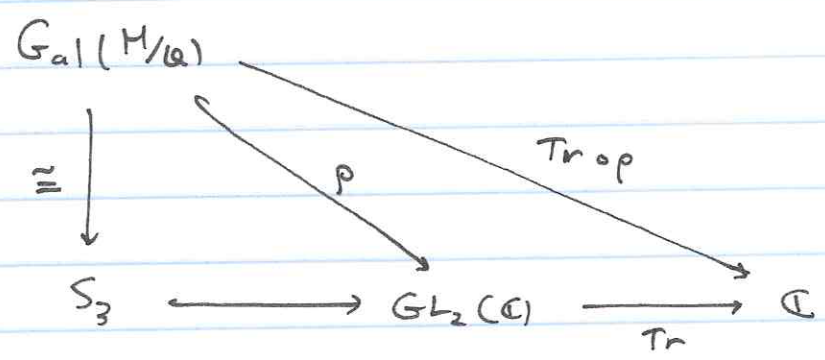
$$\frac{1}{6} \quad (\text{id})$$

Note: $M =$ Hilbert class field of $K = \mathbb{Q}(\sqrt{-23})$

$$\Rightarrow n(p) = \begin{cases} 0 & \Leftrightarrow (p) = \mathcal{O}_1, \mathcal{O}_2 \text{ w/ } \mathcal{O}_i \text{ non-principal} \\ 3 & \Leftrightarrow (p) = \mathcal{O}_1, \mathcal{O}_2 \text{ w/ } \mathcal{O}_i \text{ principal.} \end{cases}$$

$$S_3 \leftrightarrow GL_2(\mathbb{C}) :$$

			<u>order</u>	<u>trace</u>
id	\longmapsto	$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$	1	2
(123)	\longmapsto	$\begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$	3	-1
(132)	\longmapsto	$\begin{pmatrix} * & * \\ * & * \end{pmatrix}$	3	-1
(23)	\longmapsto	$\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$	2	0
(13)	\longmapsto	*	2	0
(12)	\longmapsto	*	2	0



Set $b(p) = \text{Tr}(\rho(\text{Frob}_p))$.

<u>$n(p)$</u>	<u>$f = \text{of}(\text{Frob}_p)$</u>	<u>$b(p)$</u>
0	3	-1
1	2	0
3	1	2

$n(p) = 1 + b(p)$

Recall: $f_{23}(z) = \sum a(n)q^n = \eta(z)\eta(23z) \in S_1(\Gamma_0(23), (\frac{1}{23}))$.

Thm: $n(p) = 1 + a(p)$.

Thm (Deligne-Serre 1972): Let $f = \sum a_f(m) q^m \in S_1(\Gamma_0(N), \chi)$.

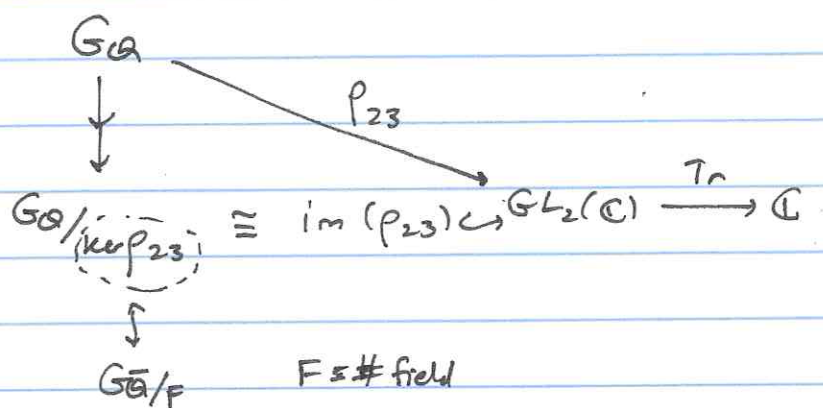
be an eigenform for all Hecke operators. Then there exists a continuous, odd, irreducible representation

$$\rho_f : \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{C})$$

s.t. $\forall p \nmid N,$

$$\text{Tr}(\rho_f(\text{Frob}_p)) = a_f(p)$$

$$\det(\rho_f(\text{Frob}_p)) = \chi(p)$$



Can then show $F = \mathbb{H}$.